

진동 큐를 이용한 스마트폰 사용자 인증 방식

이 종 혁[†] · 최 옥 경^{**} · 김 강 석^{***} · 예 흥 진^{****}

요 약

스마트폰의 특성상 이용자의 부주의로 인해 기기 및 메모리카드 등을 도난, 분실 할 수 있으며, 이에 따른 개인 정보 유출과 기업의 기밀정보 유출의 위험성이 높다. 현재 널리 사용되고 있는 스마트폰 사용자 인증방법은 개인 식별 번호 입력 방법 또는 패스워드 입력 방법이며 이것은 엿보기 공격(Shoulder Surfing Attack: SSA)에 안전하지 않기 때문에 공격자는 쉽게 사용자의 정보를 얻을 수 있다. 기존의 엿보기 공격을 막기 위한 방법으로 키스트로크 인증 방식들이 제안되어 왔으나 사용 편의성이 떨어지고 모바일 환경에서 사용하기 힘든 단점이 있다. 본 논문에서는 이러한 키스트로크 인증의 단점을 보완하기 위해 모바일 환경에 적합할 수 있도록 패스워드와 리듬 즉, 보이지 않는 null 문자를 입력하여 모바일 사용자 인증을 제한함으로써 보다 강화된 사용자 인증 서비스를 제공한다. 인증의 정확성을 높이기 위해 패턴의 규칙을 인지시켜 줄 수 있는 시각 큐와 청각 큐를 본인만 알 수 있는 템포 큐인 진동 큐를 제안하여 보안성을 강화 시킨다. 마지막으로 실험평가를 수행하여 본 연구의 효율성 및 타당성을 입증하였다.

키워드 : 키스트로크, 사용자 인증, 정보 보호, 진동 큐, 엿보기 공격

User Authentication Method using Vibration Cue on Smartphone

Jonghyeok Lee[†] · Okkyung Choi^{**} · Kangseok Kim^{***} · Hongjin Yeh^{****}

ABSTRACT

Mobile phone devices and memory card can be robbed and lost due to the carelessness that might be caused to leak personal information, and also company's confidential information can be disclosed. Therefore, the importance of user authentication to protect personal information is increasing exponentially. However, there are the limitations that criminals could easily obtain and abuse information about individuals, because the input method of personal identification number or the input method of password might not be safe for Shoulder Surfing Attack(SSA). Although various biometric identification methods were suggested to obstruct the SSA, it is the fact that they also have some faults due to the inconvenience to use in mobile environments. In this study, more complemented service for the user authentication was proposed by applying Keystroke method in the mobile environments to make up for the faults of existing biometric identification method. Lastly, the effectiveness and validity of this study were confirmed through experimental evaluations.

Keywords : Keystroke, User Authentication, Information Security, Vibration Cue, Shoulder Surfing Attack

1. 서 론

스마트폰 기기의 보편화와 대중화, 그리고 첨단화로 인해 각종 모바일 서비스들은 다양하게 증가하고 있다. 통화기능이 주 기능 이었던 모바일 기기가 이제는 이메일, 인터넷, 전자결제 등의 기능이 갖춘 소위 '내 손안의 컴퓨터'로 언제 어디서나 이용 할 수 있게 되었으며, 이에 따른 편리함과

효율성으로 인해 세계 스마트 폰 시장은 점차 증가되고 있는 실정이다[1][2].

새로운 기술이 발전이 되고 대중화가 되면 그 발전된 기술을 통해 실생활에서 적용하는 사례가 발생이 되는데 대표적으로 회사 업무에 적용 되었던 사례가 모바일 오피스이다 [3]. 모바일 오피스는 모바일 단말기를 통해 외부에서 회사 업무를 처리할 수 있어 신속한 업무환경과 편의성을 제공해준다. 하지만 개인 휴대 기기의 특성상 이용자의 부주의로 인해 기기 및 메모리카드 등을 도난, 분실 그리고 엿보기 공격(Shoulder Surfing Attack: SSA)을 통한 비밀번호 노출로 기업 및 개인정보의 유출 등 모바일 오피스 사용의 역효과가 발생하게 된다[4]. 이러한 문제점을 해결하기 위한 방안으로 생체인증 방법이 제안되어 왔다. 생체 인증은 신체의 일부분이므로 분실 위험이 적으며, 접근 카드에 비해

※ 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원사업"의 연구결과로 수행되었음.

† 준 회 원: (주)롯데정보통신 보안컨설팅팀 보안컨설팅담당 사원

** 정 회 원: 아주대학교 지식정보보안학과 연구교수(교신저자)

*** 정 회 원: 아주대학교 지식정보보안학과 연구교수

**** 종신회원: 아주대학교 지식정보보안학과 교수(교신저자)

논문접수: 2011년 12월 12일

수정일: 1차 2012년 3월 14일

심사완료: 2012년 3월 16일

상대적으로 복제나 강탈 위험이 적다는 장점이 있다. 하지만 비용, 정확성, 사용자 거부감 등과 같은 단점과 모바일 기기 적용에 대한 어려움이 발생으로 모바일 오피스의 사용자 인증에 대한 해결책으로는 한계가 있다[5].



(그림 1) SSA 엿보기 공격

본 연구에서는 생체 인식 중에서 이러한 문제를 최소화시킬 수 있는 키스트로크 인증 방식을 모바일 환경에 적합할 수 있도록 응용하여 제안함으로써 보다 강화된 사용자 인증 서비스를 제공 할 수 있도록 한다. 또한 기존의 키스트로크의 성능을 향상시키기 위해 템포 큐를 진동 큐라는 새로운 대안 방법으로 제시하였으며 SSA공격에 강력하게 대비하고, 인증의 정확성 및 강화된 점을 오인식률(FAR: False Acceptance Rate)과 오거부율(FRR: False Reject Rate), 교차 오류율(ERR: Equal Error Rate)을 실험 결과로 도출하여 그 효율성을 입증하였다[6].

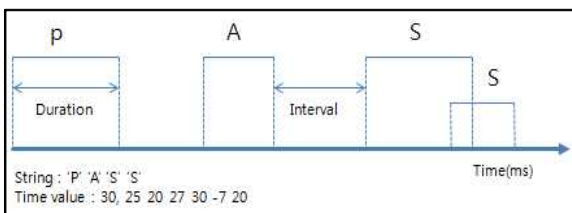
2. 관련 연구

2.1 Keystroke

키스트로크 인증 방식(Keystroke dynamic)은 사용자가 입력하는 패턴이나 습관적인 특징을 로깅하여 분석한 다음 적법한 사용자인가를 판단하여 인증하는 것을 말한다[7].

다시 말해서 키스트로크 기반의 사용자 인증은 개인마다 키스트로크 특징이 다르다는 연구 결과에 착안하여, 패스워드의 문자열뿐만 아니라, 패스워드의 키스트로크 유형까지 이용한 사용자 인증 방식이다. 즉, 패스워드 문자열이 유출되더라도 키스트로크 패턴까지 이중으로 검사하므로 공격자의 침입을 방지할 수 있게 된다[8].

‘PASS’라는 문자열을 입력하게 되면 문자열값과 입력한 시간 값이 측정되어 인증 값들이 산출된다. (그림 2)에서는 ‘P’, ‘A’, ‘S’, ‘S’라는 문자열과 30, 25, 20, 27, 30, -7, 20의 시간 값이 추출된다.



(그림 2) 키스트로크 원리

2.2 템포 큐와 인공리듬

Cho. S et al[9]의 연구에서 키스트로크 인증의 데이터의 품질은 특이도, 일관도, 변별도의 관점에서 측정하였다. 특이도는 사용자의 패턴과 침입자의 패턴이 얼마나 다른가를 판단하는 지표이며, 일관도는 사용자의 패턴과 기존 등록 한 패턴과 얼마나 비슷한가는 나타낸 지표이고, 변별도는 사용자와 침입자의 패턴 차이를 구분하는 지표이다.[9] 변별도는 실제 사용자가 인증 시스템에 인증을 시행할 때 입력한 패턴들과 침입자들이 얼마나 쉽게 구별될 수 있는지를 나타내는 개념이다. 더욱이 변별도는 특이도와 일관도의 상관관계로 설명할 수 있다[9]. 데이터의 특이도가 크면 침입자들의 입력 패턴들은 학습에 사용된 입력 패턴들과 매우 다를 것이다. 또한 데이터의 일관도가 크면, 인증을 위해 입력한 패턴들은 학습에 사용된 입력 패턴들과 매우 비슷할 것이다. 때문에 일관도와 특이도가 모두 클수록, 인증을 위해 입력한 패턴과 잠재적 침입자들의 패턴은 매우 다른 특성을 가지기 때문에 분류가 쉬워지며, 이는 높은 변별도로 설명될 수 있다[9].

변별도 또는 인증 성능을 증가시키는 방법은 두 가지가 있는데, 그것은 특이도를 증가시키거나 일관도를 증가시키는 것이다[10]. 특이도를 증가시키는 방법으로 인공리듬이 있다. 인공리듬이란 패스워드를 입력할 때 자연스럽게 입력하는 것이 아니라, 각각의 문자들을 입력하는 패턴을 미리 정하여 그 패턴에 따라서 입력하는 것이[10]. 예를 들어 “1234”라는 패스워드를 입력 할 때, 사용자가 ‘1’을 입력하고 ‘2’를 입력하기 전에 두 박자를 마음속으로 세고 입력하며, ‘2’과 ‘3’ 사이에는 한 박자를 ‘3’과 ‘4’ 사이에는 박자 없이 입력하게 되면 사용자의 입력방식은 하나의 패턴“1--2-34”이 생겨나게 된다. 사용자는 중간의 박자를 원하는 위치에 원하는 길이로 원하는 수만큼 삽입할 수 있기 때문에 이에 대한 경우의 수는 무한하다고 할 수 있다[11].

또한, 패턴의 일관도를 증가시키기 위하여 템포 큐가 제안되었다. 인공리듬을 사용하거나 패턴에 익숙하지 않은 사용자들은 패스워드를 일정하게 입력하는 것이 어렵기 때문에 일관도가 상대적으로 낮아진다. 템포 큐는 사용자가 패스워드를 입력할 때, 일정한 간격으로 사용자에게 신호를 보내주는 모든 방식을 말한다. 사용자가 자신의 입력 속도를 스스로 인지할 수 있게 하는 보조 장치로서 템포 큐를 이용하게 된다. 템포 큐란 사용자가 암호를 입력할 때 일정한 간격으로 사용자에게 신호를 보내주는 방식으로 시각 큐, 청각 큐가 있다. 시각 큐는 시각적으로 일정한 시간동안 화면을 깜박인다거나 진행 바를 두어 사용자가 템포를 인식시켜주는 손짓 역할을 하며, 청각 큐는 일정한 시간마다 비트 음을 주거나 음악을 넣어 사용자가 인식하는데 도와주는 역할을 한다[10].

2.3 기존 연구 및 분석

기존의 키스트로크 인증 방식은 양손으로 키보드를 입력하는 방식으로 양손의 입력 패턴과 리듬으로 사용자를 식별하고 구분을 하였다. 하지만 일상생활에서 컴퓨터처럼 많이 이용되고, 많은 정보를 저장하는 모바일 환경에서 이러한

인증방식을 적용하기가 어렵다. 모바일에서 패스워드 입력 방식을 양손으로 하는 경우도 거의 없으며, 짧은 패스워드를 요구하는 모바일에서 키스트로크 특징을 선별해 내는 것도 또한 쉬운 일이 아니기 때문이다. 또한 보안적인 면에서도 문제가 발생 할 수 있다. 키스트로크는 인증 성능을 향상시키기 위해 다양한 템포 큐를 사용을 하는데, 시각 큐와 청각 큐 같은 경우 화면과 소리로 공격자가 엿보기 공격으로 템포 큐의 패턴을 탐지를 할 수 있기 때문에 키스트로크의 대한 보안적 효과를 무마 시킬 수 있다. 이러한 내용들을 표현한 것이 바로 <표 1>이다.

<표 1> 기존 연구 및 분석

방식	템포 큐	단점
키스트로크 방식	시각 큐	짧은 패스워드로 인해 모바일 방식의 부적합 공격자가 엿보기 공격으로 패턴 유출 가능 타 감각 사용으로 인한 반응속도 저하
	청각 큐	
	시청각 큐	
키스트로크 방식은 키보드에서 사용하는 방식으로 짧은 패스워드 문자열과 패턴 방식을 사용하는 모바일에 적용하기에는 한계가 있다. 소리와 디스플레이가 보이기 때문에 공격자에게 패턴 유출이 충분히 가능하며 한가지 감각에 대한 반응속도에 비해 두 가지 감각을 이용 하므로 인지 반응속도가 저하되는 단점이 있다.		

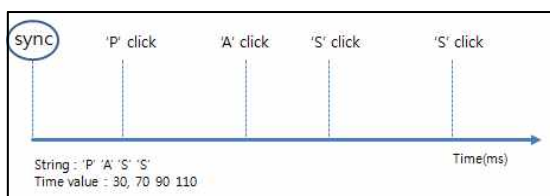
3. 설계 방안 및 구현

3.1 설계 방안

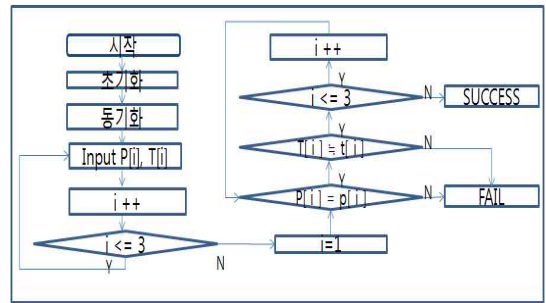
본 논문에서는 모바일 환경에서 가지는 키스트로크를 제안 하였으며 세부 내용은 다음과 같다.

먼저 Sync 키를 두어 시간 값과 템포 큐를 동기화 시켜 주고 시간 값은 Stopwatch의 원리로 문자열 하나씩 클릭을 할 때마다 시간 값을 저장 하여 각 문자열과 같이 서버에 보내게 되는 스타카토방식이다. 이때 데이터베이스에 저장해 놓은 문자열과 시간 값을 비교를 한다. 시간은 1/1000초 단위이기 때문에 인증 오차의 허용치 즉, 임계 값을 설정해 준다. 임계 값 오차 범위 내에서 문자열이 일치하였을 때 인증은 성공을 하지만 두개 요소 중에 하나라도 일치하지 않는다면 인증은 실패하게 된다.

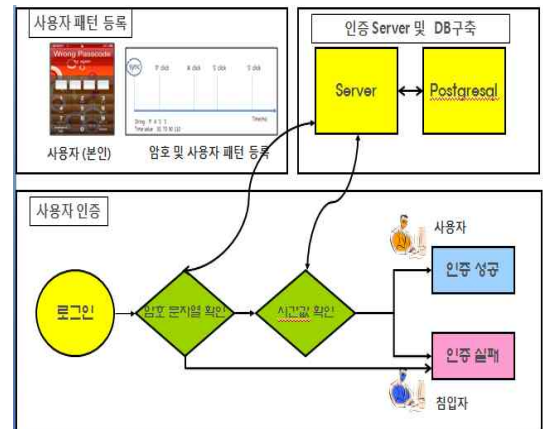
제안된 키스트로크 인증 방식으로 암호 및 사용자 패턴으로 로그인을 하게 되면 서버에서는 암호 문자열과 시간 값을 데이터베이스에 보내주어 기존의 등록했던 값들과 비교를 하게 된다. 문자열은 정확히 일치해야 하며 패턴 시간 값은 기존의 정의 해 놓은 임계 범위 안에 포함 되면 인증 성공의 필요조건이 된다.



(그림 3) 모바일의 적합한 키스트로크 방식



(그림 4) 키스트로크 알고리즘



(그림 5) 설계 구조

3.2 구현

(그림 6)을 보면 안드로이드 기반의 사용자 UI를 나타낸 것이다. 오른쪽 그림에 숫자가 있는데 그것은 시각 큐를 나타내는 것이며 나타나지 않는 그림은 시각적으로 보이지 않는 진동을 느낄 수 있는 진동 큐의 UI를 나타낸 것이다.



(그림 6) 구현 UI

구현 된 어플리케이션의 실행 방법은 다음과 같다.

특수문자 # 을 이용하여 패턴을 등록을 한다. 등록 방법은 * 버튼을 터치하여 템포 큐와 시간 값을 동기화 시켜주고 주어진 템포 큐에 맞게 자신의 패턴과 문자열을 등록을 한다. 등록이 완료가 되면 인증 페이지에서 *을 클릭하여 이벤트를 실행 시킨다. 자신이 등록한 패턴과 문자열을 입력하면 패턴의 유사도와 문자열을 등록한 값이 저장되어 있는 DB에서 비교가 되어 두 개의 인증요소가 모두 일치하

면 로그인 성공이라는 팝업 창과 더불어 동영상이 실행된다. 실패 시 서버에서 DB에서의 등록된 시간 값과 인증하기 위해 입력한 시간 값의 차이를 알려준다.



(그림 7) 동작 순서

본 논문에서 제안한 템포 큐는 진동 큐이다. 모바일에는 진동이라는 키보드와 다른 기능이 있다. 이 기능을 가지고 템포 큐로 제안 한 이유는 이러하다. 기존의 시각 큐와 청각 큐일 경우에는 엿보기 공격에 그리 안전하다고 말할 수 없기 때문이다. 공격자가 어깨 너머에서 사용자의 패스워드를 볼 때 시각적으로나 청각적으로 이러한 템포 큐와 문자열을 확인 할 수 있기 때문이다. 예를 들어서 공격자가 엿보기 공격을 할 때 사용자가 누르는 문자열은 시각적으로 확인 할 수 있는 것은 당연 할 뿐만 아니라 UI에 표현 되는 시각 큐까지 동시에 볼 수 있기 때문이다. 청각 큐 또한 소리로 나타내기 때문에 기존의 템포 큐는 그리 효과적이라고 말할 수 없다. 하지만 진동 큐일 경우에는 진동의 세기를 조절 할 수 있기 때문에 본인만 진동을 느낄 수 있어 템포 패턴을 공격자가 알아내기에 다른 템포 큐에 비해 효과적이라고 말할 수 있다.

4. 실험 평가

4.1 실험 방법

본 절에서는 다음과 같은 조건에 의해 실험 평가를 진행하였으며 자세한 사항은 다음과 같다.

- 데이터 구성을 practice의 집합으로 분류하여 추출한다.
- 서버에서 입력된 값과 등록된 값과의 오차를 알 수 있다.
- 데이터는 진동 큐, 시각 큐, 그리고 템포 큐가 주어지지 않았을 때의 3가지 상황 내에서 각각 수집 한다.
- 임계값의 오차 허용치를 변경 해주며 수집 한다.
- 템포 큐에 대한 반응속도를 측정 할 수 있도록 한다.
- 평가를 위해 사용자들에 대한 시스템 친밀도를 높이고, 시스템에 대한 정확도를 높이기 위해 몇 분간의 학습 시간을 가지고 실험을 시행한다.

- 테스트 시 실험은 진동 큐, 시각 큐가 주어졌을 때와 그리고 템포 큐가 주어지지 않는 3가지 상황과 민감도를 바꿔가며 수회 반복적 연습 후 Practice 실시하며 다음과 같은 평가 항목 산출결과를 나타낸다.

- FRR 위해 각 사용자에게 대한 genuine attempt를 수행
- FAR 위해 각 사용자에게 대한 imposter attempt를 수행

또한 제한한 실험 환경은 다음과 같다.

- ① 모든 실험은 고정 IP가 할당 된 야외환경과 필드 환경에서 진행.
 - ② 오프라인 환경에서 테스트.
 - ③ 스마트 폰을 사용하는 10세~40세 50명 대상
- 최초 Password를 등록 시 저장 된 문자열과 패턴은 DB에 저장, 이후 실험 되는 수행 값과 인증 성공여부는 서버에서 확인하여 기록표에 기입한다. (그림 8)은 실험을 측정한 데이터 기록표이다.

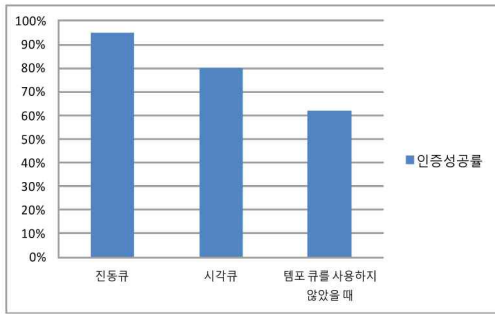
이름 : 홍길동	나이 : 28	스마트폰 사용여부: 0	비교(인증성공여부)			
성별 : (남) 여						
비밀번호 문자열 값	1	2	3	4		
비밀번호 시간벡터 값	2.034	4.556	7.321	8.011		
민감도 (고) (임계값 ±0.1초)	시각 큐	2.124	3.056	7.460	8.809	X
	진동 큐	2.034	4.455	7.229	7.989	O
	템포 큐 X	2.530	5.596	6.361	8.419	X
민감도 (중) (임계값 ±0.5초)	시각 큐	2.334	4.156	6.921	8.381	O
	진동 큐	2.634	5.036	7.621	8.411	O
	템포 큐 X	2.434	5.056	6.721	7.711	X
민감도 (저) (임계값 ±1초)	시각 큐	2.134	4.476	7.227	8.107	O
	진동 큐	2.731	4.656	7.341	7.911	O
	템포 큐 X	2.294	4.596	7.321	7.021	O

(그림 8) 실험 기록표

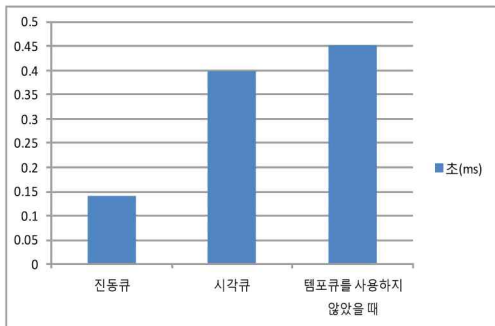
4.2 실험 결과

임계 값의 범위 0.01초~2초로 측정된 결과 인증 성공률의 대한 결과를 알 수 있다. 임계 오차 허용치가 낮을수록 인증 성공률이 낮아지는 결과가 임계 오차 허용치가 높을수록 인증 성공률은 높아지는 결과가 나왔다. 다음 (그림 9)는 0.5초의 임계 값을 기준으로 템포 큐별 인증 성공률에 대한 수치이다. (그림 10)은 템포 큐에 따른 오차 평균에 대한 수치이다. 측정된 결과 진동 큐가 다른 대조군들에 비해 인증 성공률이 높다는 결과와 반응속도가 빠르다는 것을 볼 수 있다. 이러한 결과가 나온 이유로는 시각 큐는 눈으로 보고 박자를 세는 것에 비하여 진동 큐는 직접 촉각으로 느끼기 때문에 그에 대한 반응속도가 빠른 것으로 판단된다.

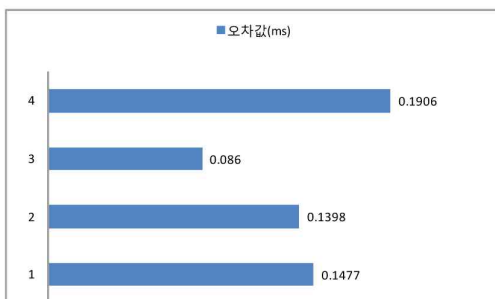
모든 템포 큐에 대하여 인증 하는데 있어서 첫 번째 키부터 네 번째 키까지 오차의 차이가 가장 적은 키를 분석하였다. 그 결과 각 문자열마다의 평균 오차 값은 (그림 11)과 같은 결과가 나타난다.



(그림 9) 템포 큐에 따른 인증 성공률



(그림 10) 템포 큐에 따른 오차 평균값



(그림 11) 키 순서에 따른 오차 평균값

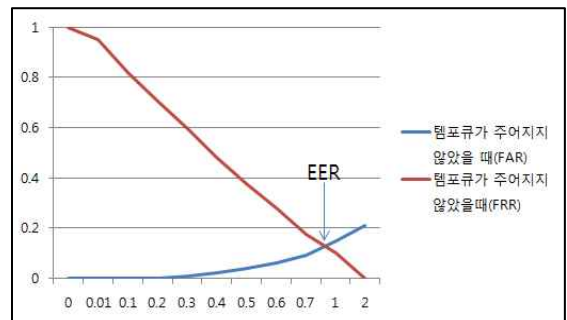
이러한 결과가 나왔던 것은 첫 번째 키에서 세 번째 키까지 터치함에 있어서 점차 템포 큐에 적응이 되어 혹은 자신만의 박자에 적응이 되어서 점차 오차 값이 줄어들게 되지만, 마지막 키에서는 마지막 터치라는 생각으로 집중이 떨어져서 가장 큰 오차 값이 나타난 것이라고 예상된다.

오인식률(FAR: False Acceptance Rate)과 오거부율(FRR: False Reject Rate)은 개인을 식별하는 생체인식 기술의 수준을 평가하는데 쓰는 용어들이다. 오인식률이란 다른 사람의 생체인식 정보를 특정인의 것으로 잘못 인식할 수 있는 비율을 말하는 것이며 오인식률만 가지고 시스템 성능을 판단하면 매칭 수준을 지나치게 엄격히 함에 따라 잘못 인식하는 비율은 낮아지지만 인증을 거부하는 비율이 높아져 사실상 시스템 사용에 문제가 발생할 가능성이 있다 이 때문에 항상 오거부율과 함께 거론된다. 오거부율이란 시스템이 개인을 식별할 때 잘못 거부하는 비율을 말한다. 오거부율이 높으면 실제 생체인식 정보의 주인이 통과하려 할 때도

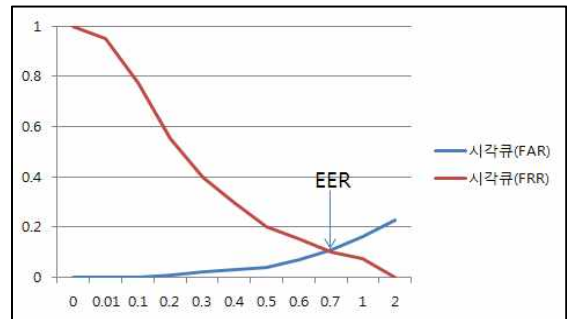
이를 거부하기 때문에 아무리 보안 수준이 높아진다고 해도 실제로 사용하는데 불편함이 많아진다.

오인식률과 오거부율이 그래프상 만나는 점을 교차 오류율(ERR)이라 한다. 이것은 인증 시스템의 평가 요소로써 이 오류율이 낮을수록 좋은 시스템이라고 평가 되고 있다[10].

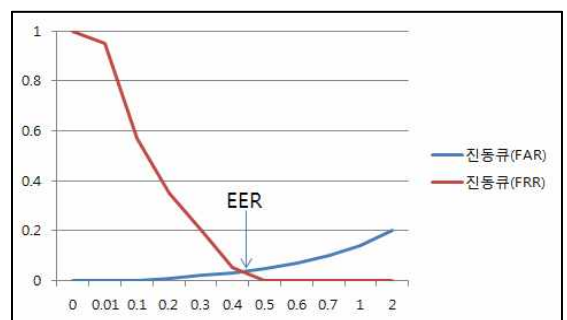
본 논문에서는 오인식률과 오거부율을 측정을 하고 이에 대한 교차 오류율을 측정함으로써 제안하고자 하는 진동 큐에 대한 성능평가를 수행하고자 한다. 진동 큐와 시각 큐, 그리고 템포 큐를 사용하지 않았을 때의 교차 오류율은 다음 그림과 같다.



(그림 12) 템포 큐를 사용하지 않았을 때 오류율



(그림 13) 시각 큐를 사용하였을 때 오류율



(그림 14) 진동 큐를 사용하였을 때 오류율

<표 2> 템포 큐별 교차 오류율 값

without 템포 큐	시각 큐	진동 큐
0.16%	0.1%	0.06%

템포 큐를 사용하지 않았을 때의 교차 오류율은 0.16%가 나타났으며 시각 큐를 사용할 때는 0.1%, 진동 큐를 사용할 때는 0.06%로 전체적인 교차 오류율의 값이 진동큐를 사용했을 때 가장 낮은 결과를 볼 수 있다. 따라서 성능 평가 결과 진동큐가 가장 우수하다는 것을 증명할 수 있었다.

5. 결 론

본 논문에서는 진동 큐를 이용하여 스마트 폰 사용자 인증 방식에 대해서 제안을 하였다. 모바일 사용자 인증의 성능을 향상시키기 위한 방법으로 패스워드 뿐만 아니라 리듬, 즉 보이지 않는 시간 null 문자를 인증하는데 사용하였으며, 기존의 SSA 공격에 취약한 기존의 템포 큐(시각 큐, 청각 큐, 시청각 큐)와 달리 모바일에서는 촉각으로 느낄 수 있는 촉각 큐, 즉 진동 큐를 추가적으로 사용하여 보안성을 강화시켰다. 본 논문에서는 진동 큐의 일관성과 정확성을 측정하는 시험을 하여, 기존의 템포 큐와 비교 분석을 하였으며 그 결과 진동 큐 같은 경우에는 시각이나 청각과 달리 진동이 촉각으로 느끼므로 반응속도가 빨라져 정확도, 일관성에 대해서 긍정적인 영향을 미치는 결과를 알 수 있었다. 향후 연구과제로 사용자가 이동 중에 본 논문에서 제안하는 진동 큐를 이용한 사용자 인증을 수행 할 때 효율적이고 타당한지에 대한 실험 평가를 수행해 봄으로써 모바일 환경에 적합하고 강력한 보안 인증 방식인지 여부를 증명해 보이고자 한다.

참 고 문 헌

[1] 나성욱, "스마트 폰과 모바일 오피스의 보안 이슈 및 대응 전략", CIO Report Vol.26, 한국정보화진흥원, 2010. 10.
 [2] 방송통신위원회, 한국인터넷진흥원, "스마트 폰 이용 실태 조사(II)", pp.22, 2010년 12월.
 [3] 삼성경제연구소, "모바일 빅뱅이 촉발하는 기업경영의 변화", Issue Paper, 2010년 10월.
 [4] 강동호, "스마트 폰 보안 위협 및 대응 기술", 전자통신동향분석 제 25권 제 3호, 2010년 6월.
 [5] 전명근, "생체정보 이용과 프라이버시 보호", 한국정보보호학회 지 제 15권 제 6호, 2005년 12월.
 [6] Hopkins, R, "An Introduction to Biometrics and Large Scale Civilian Identification," International Review of Law Computer and Technology, Vol.13, No.3, pp.337-363, 1999.
 [7] 황성섭 "키스트로크 다이내믹스 분석을 이용한 모바일 사용자 인증", 한국경영과학회 2006년 추계학술대회논문집, pp.652-655, 2006.11
 [8] 김천식 "이러닝 시스템에서 사용자 인증을 위한 키스트로크의 응용 기술", 전자공학회논문지-CI 제 45권 제 5호 (통권 제 323호), pp.25-31, 2008년 9월.
 [9] Cho, S. and Hwang, S. "Artificial rhythms and cues for keystroke dynamics based authentication", Lecture Notes in Computer Science (LNCS), Vol.3832, pp.626-632, 2005.

[10] Hwang, S., Lee, H. and Cho, S. "Improving authentication accuracy using artificial rhythms and cues for keystroke dynamics-based authentication", Expert Systems with Applications, Vol.36, pp.10649-10656, 2009.
 [11] Coventry, L., A. De Angeli, and G.Johnson, "Usability and Biometric Verification at the ATM Interface," SIGCHI conference on Human factors in computing systems, pp.153-160, 2003.



이 종 혁

e-mail : yahssap@ajou.ac.kr
 2012년 아주대학교 지식정보보안학과 (공학석사)
 2012년~현 재 (주)롯데정보통신 보안 컨설팅팀 보안컨설팅담당 사원
 관심분야: Mobile Security, Financial Security, User Authentication



최 옥 경

e-mail : okchoi@ajou.ac.kr
 2006년 중앙대학교 컴퓨터공학과(공학박사)
 2011년~현 재 아주대학교 지식정보보안학과 연구교수
 관심분야: Semantic Web Services System, e-Commerce, Auction, Information Retrieval, Mobile Cloud Computing Security, Mobile/Wireless Network Security



김 강 석

e-mail : kangskim@ajou.ac.kr
 2007년 인디애나 대학교 컴퓨터공학과 (공학박사)
 2010년~현 재 아주대학교 지식정보보안학과 연구교수
 관심분야: mobile computing, ubiquitous computing, scalable distributed database system, floor control, mobile applications with smart phones, mobile security, data mining and bioinformatics



예 흥 진

e-mail : hjyeh@ajou.ac.kr
 1993년 Universite Joseph Fourier-Ecole Normale Supérieure de Lyon (France), 공학박사(전자계산학)
 1993년~현 재 아주대학교 정보컴퓨터공학부 부교수
 관심분야: Information Security, Mobile Security, Application Security