키스트로크 다이나믹스 분석을 이용한 모바일 사용자 인증[1)]

Mobile User Authentication using Keystroke Dynamics Analysis

황성섭*, 조성준*, 박성훈*

* 서울대학교 (hss9414@snu.ac.kr, zoon@snu.ac.kr, shpark82@snu.ac.kr)

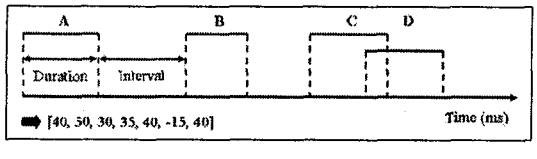
Abstract

최근 핸드폰 같은 휴대용 단말기의 용도는 통화 이외에도 예금, 증권, 결제, 신원확인 등과 같은 다양한 어플리케이션으로 발전하고 있다. 본 논문에서는 키스트로크 기반의 사용자 인증을 이용한 모바일 보안강화 방안에 대하여 논의한다. 키스트로크 다이나믹스 패턴분석은 사용자가 특정 문자열을 타이핑할 때의 입력 패턴을 고려한 분석 방법이다. 본 연구는 휴대단말기의 짧은 암호사용의 문제점을 극복하기 위하여 인공리듬과 템포 큐를 활용하였으며, 높은 분류 성능을 보여주었다.

1. 서론

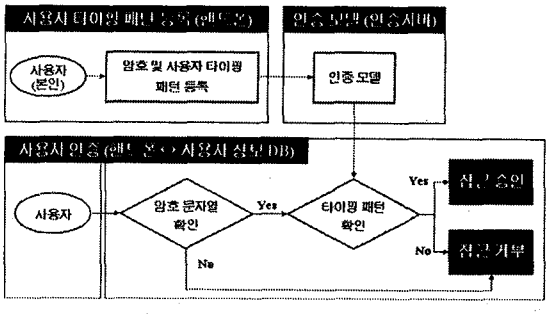
최근 모바일 보안의 중요성은 증대하고 있다. 특히 핸드폰과 모바일 기기는 단순한 통신의 수단이 아니라 예금, 증권, 결제, 신원확인 등과 같은 다양한 형태의 어플리케이션을 가지고 있기 때문이다 (Clarke et al, 2002). 휴대용 단말기에 지문, 홍채, 음성 등의 생체인식 방법들이 활용되고 있지만, 여전히 비용, 정확성, 사용자 거부감 등의 문제가 남아 있다(Boertien and Middelkoop, 2002; Clarke and Furnell, 2005).

키스트로크 다이나믹스 패턴분석(Gaines et al, 1980; Umphress and Williams, 1985)은 사용자가 특정 문자열을 타이핑할 때의 입력 패턴을 고려한 분석 방법이다. 예를 들어, 사용자가 'ABCD'라는 문자열을 타이핑할 때, ms(millisecond) 단위로 7개의 시간 값이 측정되어 [그림 1]과 같은 7차원 타이밍 벡터를 산출한다.



[그림 1] 문자열 "ABCD"의 타이핑 패턴

키스트로크 다이나믹스 기반의 사용자 인증은 개인마다 키스트로크 패턴이 다르다는 연구결과에 착안하여, 암호의 내용뿐만 아니라, 암호의 키스트로크 패턴까지 이용한 사용자 인증 방식이다. 즉, 암호가 유출되어 일차적인 보안망을 통과하더라도 키스트로크 패턴까지 검사하여 침입을 방지할 수 있다. 이러한 키스트로크 다이나믹스 패턴분석은 허가받지 않은 사용자의 무단접근 또는 해킹을 방지하기 위한 수단으로 자주 사용된다. Clarke et al.(2003)는 단말기 보안을 위하여 키스트로크 분석을 연구하였으나 단말기 자체의 보안에 국한되어 있어서, 무선 서비스에의 응용까지는 진행되지 않은 상황이다. 키스트로크 기반의 모바일 사용자 인증은 [그림 2]와 같이 (1) 사용자 타이핑 패턴 등록, (2) 인증모델 구축, (3) 사용자 인증 과정을 거친다.



[그림 2] 키스트로크 기반의 모바일 사용자 인증

키스트로크 기반의 사용자 인증의 어려운 점은, 패턴인식 관점에서 볼 때, 모델 구축 시에 침입자의 패턴이 가용하지 않다는 것이다. 따라서 이진분류(binary classification) 문제로 학습이 불가능하기 때문에, 이상탐지(novelty detection) 문제로 접근해야 한다(Cho et al., 2000; Yu and Cho, 2004). 기하학적인 관점에서, 이상탐지 모델은 정상 패턴 주변에 닫힌 경계를 생성한다(Japkowicz, 2001). 또 다른 문제는 사용자 패턴의 수가 제한적이라는 점에서 기인한다. 사용자 입력 패턴의 수가 많을수록 인증 정확도는 높아지지만, 수백 개의 패턴을 등록하는 것은 비현실적이다. 또한 휴대단말기처럼 비교적 짧은 암호를 사용하는 경우 더더욱 성능은 떨어지기 쉽다. 최근 타이핑 패턴의 품질, 다시 말해, 패턴의 특이도(Uniqueness)와 일관도(consistency), 변별도(discriminability)를 증가시키기 위하여 인공리듬

1) 본 논문은 한국과학재단의 특정기초연구과제(과제번호 R01-2005-000-10390-0)와 2단계 BK21 사업의 지원으로 이루어졌습니다.

(artificial rhythm)과 템포 큐(tempo cue)가 제안되었다(Cho and Hwang, 2006). 본 연구는 휴대용 단말기의 짧은 암호 사용의 문제점을 극복하기 위하여 인공리듬과 템포 큐를 활용하였다.

논문은 다음과 같이 구성되어 있다. 다음 장에서는 모바일 사용자 인증 모델을 설명하고, 3장에서 데이터 수집 과정과 관련 프로그램에 대하여 서술할 것이다. 최종적으로 실험결과와 결론을 제시할 것이다.

2. 모바일 사용자 인증 모델

2.1 데이터 품질

키스트로크 기반의 사용자 인증에서 데이터의 품질은 특이도, 일관도, 변별도의 관점에서 측정될 수 있다. 특이도는 유효한 사용자의 패턴이 잠재적인 침입자의 패턴과 얼마나 다른가와 관련되고, 일관도는 등록 단계에서의 사용자 패턴과 인증 단계에서의 패턴이 얼마나 유사한가를 나타낸다. 최종적으로 변별도는 사용자의 패턴과 침입자의 패턴을 얼마나 잘 구분해낼 수 있는가와 관련되는 것이다.

$\{\overrightarrow{x_i}|i=1,\cdots,N_x\}$, $\{\overrightarrow{y_j}|j=1,\cdots,N_j\}$, $\{\overrightarrow{z_k}|k=1,\cdots,N_z\}$을 각각 등록 타이핑 패턴, 유효한 사용자의 로그인 패턴, 침입자의 패턴이라고 하자. 프로토타이프 $\overrightarrow{m}$을 $\overrightarrow{m}=\sum_{i=1}^{N_x}\overrightarrow{x}/N_x$로 정의할 때, 타이핑 패턴의 품질 척도는 다음 [그림 3]와 같이 정의할 수 있다.

$$Uniqueness=\sum_{k=1}^{N_z}\frac{|\overrightarrow{z_k}-\overrightarrow{m}|}{N_z}-\sum_{i=1}^{N_x}\frac{|\overrightarrow{x_i}-\overrightarrow{m}|}{N_x}$$

$$Inconsistency=\sum_{j=1}^{N_y}\frac{|\overrightarrow{y_j}-\overrightarrow{m}|}{N_y}-\sum_{i=1}^{N_x}\frac{|\overrightarrow{x_i}-\overrightarrow{m}|}{N_x}$$

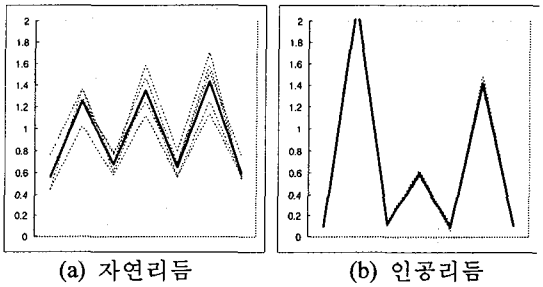
$$Discriminability=\min_{\forall k}|\overrightarrow{z_k}-\overrightarrow{m}|-\max_{\forall j}|\overrightarrow{y_j}-\overrightarrow{m}|$$

[그림 3] 타이핑 패턴의 품질 척도

2.2 인공리듬과 템포큐

변별도 또는 인증 성능을 증가시키는 방법은 두 가지가 있는데, 그것은 특이도를 증가시키거나 일관도를 증가시키는 것이다. 먼저 특이도를 증가시키는 방법으로 인공리듬이 제안되었다. 인공리듬이란 패스워드를 입력할 때 자연스럽게 입력하는 것이 아니라, 각각의 문자들을 입력하는 방식을 미리 정하여 그 방식에 따라서 입력하는 것을 말한다. 예를 들어, "5805"라는 암호를 입력할 때, 사용자가 '5'를 입력하고 '8'를 입력하기 전에 세 박자를 마음속으로 세고 입력하며, '0'와 '5' 사이에 동일한 방식으로 두 박자의 포즈(pause)를 삽입한다면, 이 사용자의 암호 입력방식은 "5___80__5"가 된다. 사용자는 포즈를 원하는 위치에, 원하는 길이로, 원하는 수만큼 삽입할 수 있기 때문에, 가능한 방식은 무한히 많다고 할 수 있다. 아래 [그림 4]는 암호 "5805"를 자연리듬(a)과 인공리듬(b)의 두 가지로 입력한 패턴의 타이밍 벡터[2]를 나타낸 것이다.

또한, 패턴의 일관도를 증가시키기 위하여 템포 큐가 제안되었다. 인공리듬을 사용하거나 타이핑에 익숙하지 않은 사용자들은 등록 패턴을 일정하게 입력하는 것이 어렵기 때문에, 일관도가 상대적으로 낮아진다. 템포 큐는 사용자가 암호를 입력할 때, 일정한 간격으로 사용자에게 신호를 보내주는 모든 방식을 말한다. 사용자가 자신의 입력 속도를 스스로 조절할 수 있게 하는 보조 장치로서 템포 큐를 이용하게 된다. 템포 큐는 크게 시각적 효과를 주는 시각 큐(visual cue), 청각적 효과를 주는 청각 큐(auditory cue), 시청각 큐(audiovisual cue)의 세 가지로 나눌 수 있다.



(a) 자연리듬 (b) 인공리듬

[그림 4] 자연리듬과 인공리듬

2.3 인증모델

먼저, 두 타이핑 패턴 x_i와 x_j 사이의 거리는 다음 식 (1)과 같이 구할 수 있다.

$$dist(x_i,x_j)=\sqrt{\frac{(x_i-x_j)^T(x_i-x_j)}{d}} \quad (1)$$

여기서 d는 타이밍 벡터의 차원수이다. 사용자는 타이핑 전략으로 자연리듬과 인공리듬을 사용할 수 있기 때문에, 같은 암호라 할지라도 input scale에 차이가 날 수 있다. 이에 따른 효과를 보상해 주기 위하여 norm-factor를 다음 식 (2)과 같이 정의한다.

$$|x|_2=\sqrt{\frac{x^Tx}{d}} \quad (2)$$

Step 1: Find the prototype
$P=mean(x_i), i=1,\cdots,n$

Step 2: Decision Making
If $\dfrac{dist(y,P)/|P|_2}{\frac{1}{n}\sum_{i=1}^{n}dist(x_i,P)/|P|_2}<\theta$, accept
else reject

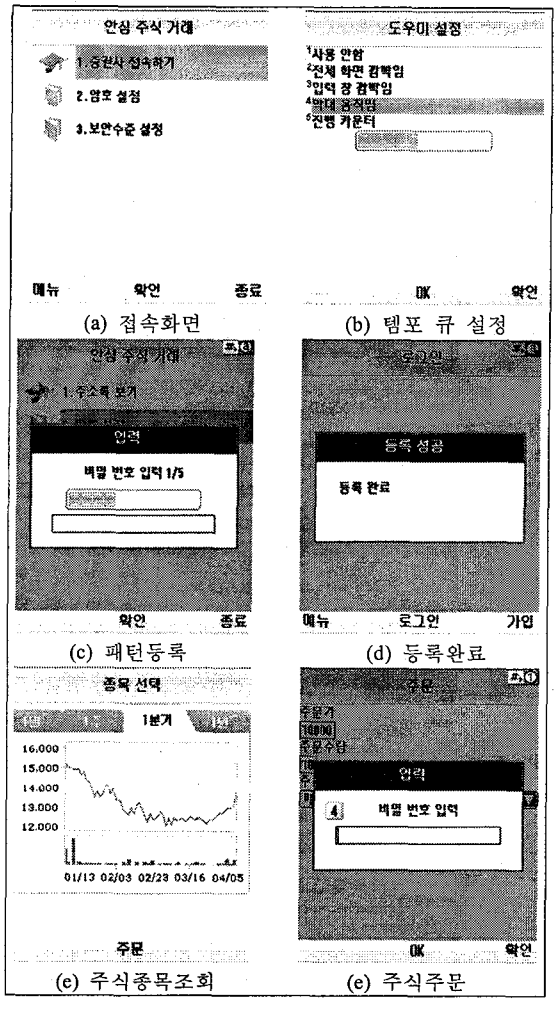
[그림 5] 인증 프로세스

인증모델에서 테스트 패턴 y가 인증되는 프로세스는 [그림 5]와 같다. 최적의 threshold parameter를 찾기 위한 threshold θ의 값은 1.0~4.0까지 0.2 단위로 증가시켜 가면서 분석하였다.

2) [그림 4]의 타이밍 벡터는 실제 측정값(ms 단위)을 식 (2)의 norm factor로 보정한 값을 나타낸 것이다. 점선은 등록 패턴, 실선은 등록 패턴의 프로토타이프를 나타낸다.

3. 데이터 수집

실험에 사용한 데이터는 2006년 6월에, 22세에서 33세(평균연령:25.3세)까지 25명의 대학원생으로부터 수집되었다. 실험을 수행한 단말기 모델은 삼성전자 SCH-V740이고, 이동통신사는 SK Telecom의 서비스를 이용하였다.



[그림 6] 주식거래를 위한 보안접속 메뉴

실험을 수행하기 전에 간단한 설문조사를 실시하였는데, 그 내용은 다음과 같다. 먼저 핸드폰 암호 입력 시, 실험자들의 약 68%는 양손으로, 나머지 32%는 한손으로 입력하였다. 실험자들이 현재의 암호를 설정한 이유는 44%가 생일, 전화번호, 주민번호 등의 친근한 숫자이기 때문이고, 32%는 키패드의 배열을 고려할 때 입력이 용이하기 때문이라고 대답하였다. 이러한 설문내용을 토대로 비교해 볼 때, 4자리 숫자 암호의 조합이 10,000개이고, 유추하기 쉽기 때문에 인공리듬의 사용이 매우 필요하다는 동기가 될 수 있을 것이다.

실험은 가상의 증권 사이트에 접속해서 주식거래를 하는 시나리오로 수행되었으며, 구현된 프로그램은 [그림 6]과 같다. 주식거래 메뉴를 통하여 증권사에 접속하여 주가를 조회하거나 매매를 할 수 있도록 되어있다. 인공리듬은 사용자가 자유롭게 결정할 수 있으며, 템포 큐[3]는 [그림 6(b)]와 같이 다양한 종류를 선택가능하게 하였다.

데이터는 자연리듬과 인공리듬으로 나누어 각각 수집하였다. 25명의 사용자는 각각 5개씩 자신의 패턴을 등록하고, 등록데이터와는 별개로 30번의 로그인을 시도하였다. 또한, 각 사용자는 자신을 제외한 나머지 24명의 암호에 대하여 2번씩(총 48회)의 해킹을 시도하였다. (단, 패스워드의 길이는 4자리 숫자로 통일하였다.) 자연리듬과 인공리듬 모두 같은 암호를 사용하였으며, 각 사용자의 수집 패턴 수 및 암호는 다음 <표 1>과 같다.

<표 1> 수집 패턴 수 및 사용자 암호

	등록	로그인	해킹
자연리듬	5	30	48
인공리듬	5	30	48

(a) 수집 패턴 수

ID	암호	ID	암호	ID	암호
01	1223	10	3784	19	2580
02	3143	11	3579	20	2220
03	0083	12	1379	21	1133
04	1472	13	0822	22	1258
05	7118	14	4569	23	5262
06	7265	15	0203	24	1125
07	2385	16	1004	25	0305
08	5805	17	5472		
09	2580	18	3887		

(b) 사용자의 암호

4. 실험결과

분류 또는 탐지 모델은 [그림 7]과 같이 두 가지 종류의 에러, false acceptance error (FAR)와 false rejection error (FRR)를 가진다(Golarelli et al, 1997; Fawcett, 2006). 계정공유의 탐지에 있어서, FRR은 오경보(false alarm)로, FAR은 누락(miss)으로 생각할 수 있다. 탐지의 기준인 threshold가 변함에 따라 하나의 에러가 증가하면 다른 하나의 에러가 감소하기 때문에, 우리는 equal error rate(EER)로서 모델의 성능을 측정하였다. 여기서 EER은 FAR과 FRR이 같아지는 지점이다.

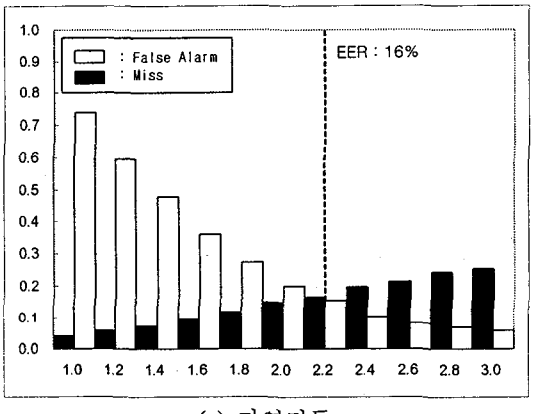
		True class: p	True class: n
Hypothesized class	Y	True Positive	False Positive
	N	False Negative	True Negative
Column totals		P	N

[그림 7] Confusion Matrix

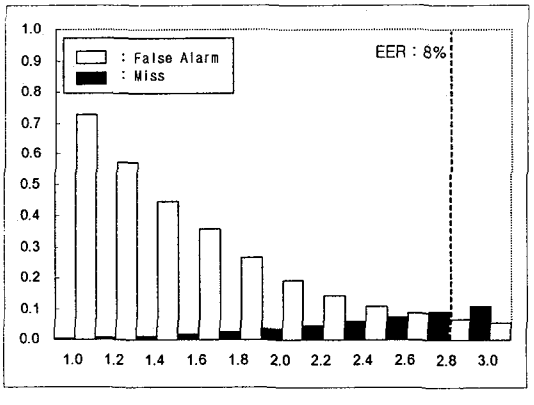
자연리듬으로 타이핑한 사용자 패턴의 인증 결과는 [그림 8(a)]와 같으며, threshold θ가 2.2일 때, EER 16%를 나타내었다. 반면, 인공리듬을 이용한

3) 템포 큐의 속도는 500ms으로 고정하였다.

실험결과는 [그림 8(b)]와 같으며, threshold θ가 2.8일 때, EER 8%를 나타내었다. 인공리듬을 사용함으로써 EER은 자연리듬을 사용한 경우의 절반 수준으로 떨어지는 것을 볼 수 있다. 타이핑 전략을 인공리듬으로 사용한 경우의 성능을 살펴보면, 포즈를 삽입한 횟수나 길이가 증가할수록 타이핑 패턴의 품질이 향상되어 높은 사용자 인증 성능을 나타내었다.



(a) 자연리듬



(b) 인공리듬

[그림 8] 사용자 인증 결과

개별적인 사용자의 실험결과를 살펴보기로 하자. 전체 25명의 사용자 중에서 17명의 인증 성능이 향상되었고, 나머지 8명의 인증 성능은 감소되었다. 흥미로운 사실은, 인공리듬을 사용함으로써 성능이 감소된 사용자는 자연리듬 정확도가 매우 높은(93.26%) 사람들인 반면, 인공리듬을 사용함으로써 성능이 증가한 사람들은 자연리듬 성능이 비교적 낮은(79.67%) 사용자들이라는 점이다. 이것은 자연리듬의 타이핑 패턴의 품질이 높은 사람들은 자연리듬 자체로도 좋은 성능을 보여줄 수 있다는 것이며, 반대로 타이핑 패턴의 품질이 낮은 사람들에게 인공리듬의 사용이 더 효과적이라는 것을 보여준다.

5. 결론

최근 핸드폰 같은 모바일 단말기는 기본적인 통화 목적에서 예금, 증권, 결제, 신원확인 등과 같은 다양한 어플리케이션으로 발전하고 있다. 본 논문에서는 키스트로크 기반의 사용자 인증을 이용한 모바일 보안강화 방안에 대하여 논의하였다. 본 연구는 휴대단말기의 짧은 암호 사용의 문제점을 극복하기 위하여 인공리듬과 템포 큐를 활용하였으며, 높은 분류 성능을 보여주었다.

추후연구는 다음과 같다. 먼저, 키패드, 키보드 등의 다양한 입력기기의 특성에 대하여 비교연구가 진행되어야 할 것이다. 또한, 다양한 연령대와 여러 가지 형태의 모바일 기기에 대한 실험이 수행되어야 할 것이다.

참고문헌

Boertien, N., Middelkoop, E. (2002), "Authentication *in mobile applications*," Technical Report.

Cho, S. and Hwang, S. (2006), "Artificial Rhythms and Cues for Keystroke Dynamics-based Authentication," Lecture Notes in Computer Science, **3832**, 626-632.

Cho, S., Han, C., Han, D. and Kim, H. (2000), "Web Based Keystroke Dynamics Identity Verification Using Neural Networks," Journal of Organizational Computing and Electronic Commerce, **10**(4), 295-307.

Clarke, N., Furnell, S., Rodwell, P.M. and Reynolds, *P.L. (2002), "Acceptance of Subscriber* Authentication Methods For Mobile Telephony Devices," Computers & Security, **21**(3), 220-228.

Clarke, N., Furnell, S., Lines, B. and Reynolds, P. (2003), "Using keystroke analysis as a mechanism for subscriber authentication on mobile handsets," In: Proceedings of IFIP SEC 2003, Athens, Greece, 26-28 May 2003. 97-108.

Clarke, N. and Furnell, S. (2005), "Authentication of users on mobile telephones - A survey of attitudes and practices," Computers & Security, **24**(7), *519-527.*

Fawcett, T. (2006), "An introduction to ROC analysis," Pattern Recognition Letters, **27**(8), 861-874.

Gaines, R., Lisowski, W., Press, S. and Shapiro, N. (1980), "Authentication by keystroke timing: some preliminary results," Rand Report R-256-NSF, Rand Corporation.

Golarelli, M., Maio, D. and Maltoni, D. (1997) "On the Error Reject Trade-off in Biometric Verification Systems," IEEE Transactions on Pattern Analysis and Machine Intelligence, **19**(7), 786-796.

Japkowicz, N. (2001), "Supervised versus Unsupervised Binary learning by Feed-forward Neural Networks," Machine Learning, **42**(12), 97-122.

M. Golarelli, D. Maio, and D. Maltoni, "On the Error Reject Trade-off in Biometric Verification Systems," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 786-796, 1997.

Umphress, D. and Williams, G. (1985), "Identity Verification through Keyboard Characteristics," International Journal of Man Machine Studies, **23**, 263-273.

Yu, E., Cho, S., (2004), "Keystroke Dynamics Identity Verification - Its Problems and Practical Solutions," Computer and Security, **23**(5), 428-440.