사 방향 기반 버튼 압력 값을 활용한 인증 방식의 보안성 연구

D-pad Based Authentication Method with Binary Pressure

추두연
DooYeon Chu
연세대학교
인지과학협동과정
Graduate Program in Cognitive Science, Yonsei University
yapchu@gmail.com

김명아
MyoungAh Kim
연세대학교
인지과학협동과정
Graduate Program in Cognitive Science, Yonsei University
makjn4029@gmail.com

김세이
Sei Kim
연세대학교
정보대학원
Graduate School of Information, Yonsei University
sayasaday@gmail.com

홍수미
Sumi Hong
연세대학교
정보대학원
Graduate School of Information, Yonsei University
hsum55555@gmail.com

조광수
Kwangsu Cho
연세대학교
정보대학원,
인지과학협동과정
Graduate School of Information, Graduate Program in Cognitive Science, Yonsei University
kwangsu.cho@gmail.com

요약문

이 연구는 리모트 컨트롤의 사 방향 키를 활용한 이용한 개인 인증 방식에 대한 보안성을 확인하는 것이다. 스마트티비를 포함한 스마트 디바이스에서 개인 인증을 위해 자주 사용되는 PIN(Personal Identification Number)의 엿보기 공격에 대한 취약성을 강화하기 위해 4 방향 PIN 방식 패턴에 두 단계의 압력을 추가하였다. 강,약의 두 단계의 압력 단계만을 추가하여 엿보기 공격 실험을 통해 확인한 결과 엿보기 공격에 대한 방어가 강화되는 것을 확인할 수 있었고, 패스워드 유출도 정도에 대한 검증을 통해 압력에 대한 보안 강화 정도를 확인할 수 있었다.

주제어

Finger Pressure Force , 개인 인증, 생체 인증, 엿보기 공격, 리모컨 인터랙션

1. 서 론

인터넷의 보급과 스마트 디바이스의 증가로 인해 인터넷 기술을 통한 온라인 서비스들이 폭발적으로 성장하고 있다. 이런 서비스들은 사용자에게 패스워드 기반의 인증을 요구하는데 이때 입력을 요구하는 패스워드 인증은 가장 흔한 사용자 인증 방식으로 사용된다.[1] 하지만 사람들은 복잡한 패스워드를 기억하기 힘들어 하기 때문에 간단하고 약한 수준의 패스워드를 사용하곤 하는데 이런 패스워드는 보안에 있어서 상당히 취약할 수밖에 없다. 이런 취약한 패스워드는 유출을 통하여 침입자에게 거짓 인증을 가능하게 만들고 있다. [2]

스마트 디바이스의 하나인 스마트 TV 의 활용도 또한 다양하게 변하고 인터넷이 연결되면서 그 안에서 제공되는 서비스 또한 다양해지고 있다. 신규 서비스를 포함해 기존에 존재하던 인터넷 서비스가 TV 에서 사용자들이 접근할 수 있게 된 것이다. 이에 따라 TV 에서도 역시 사용자 인증을 통한 서비스 제공을 요구하고 있다.

하지만 TV 는 기존의 PC 기반이나 모바일 기반의 서비스의 접근과는 다른 환경이기 때문에 보안에 대한 다른 접근 방식이 필요하다. 현재 TV 에서 가장 많이 사용되고 있는 사용자 인증 방식은 숫자 4 자리로 구성된 사용자 식별 번호(Personal Identification Number-PIN)가 주이다. 이 때 요구되는 PIN 입력 상황은 모바일 기기나 ATM 기기와 같이 기존에 PIN 을 입력해야 하는 상황과 비교할 때 몇가지 제약 조건이 따른다.

TV 의 제약 조건으로는 첫째, TV 는 리모컨을 사용하기 때문에 입력 방식에 제한이 있다. 모바일 기기나 ATM 기기와 같은 기존 PIN 입력 환경에서는 키보드 혹은 터치 스크린 등을 사용하여 숫자를 입력하는데 불편함이 없지만, TV 의 경우 리모컨을 통해서만 입력이 가능하다는 제약이 있다. 물론 모바일 연동이나 통합 ID 방식이 존재하지만 이것이 근본적인 문제에 대한 해결이 될 수 없고 이 또한 사용자에게 불편함을 불러오는 행위이다. 특히

제조사에 제조하는 리모컨에는 서비스의 의도와 다르게 제작되는 경우가 많으므로 이런 제약은 더욱 커질 수 밖에 없다. 그 예로 유일한 입력 장치인 리모컨의 숫자 버튼을 없애고 방향키를 포함해 몇가지 주요 핫 키만 남는 형태로 점차 간소화되고 있기 때문에 PIN 입력에 있어서 문제가 심각하다. 이런 상황이다 보니 각 서비스들은 각자의 PIN 을 입력할 수 있는 온스크린키보드(On-Screen Keyboard : OSK)를 자체적으로 지원하는 방식으로 가고 있다.

둘째, TV 는 다른 스마트 디바이스에 비해 엿보기 공격에 매우 취약한 특성을 가지고 있다. TV 는 디바이스 특성 상 다른 사람이 엿보기 쉬운 공개적인 디스플레이를 가지고 있고 리모컨을 이용한 입력 외의 수단이 없기 때문에 키보드 등을 이용한 PC 패스워드에 비해 그 보안성이 약할 수밖에 없다. 게다가 앞에서 언급한 OSK 를 사용한 인증 방식은 공개된 장소에서 여러 명이 공유하는 특징으로 인해 사용자 인증 과정에서 엿보기 공격(Shoulder surfing attack)의 위험이 있다. 엿보기 공격이란, 사용자의 PIN 입력 장면을 어깨너머로 관찰하여 PIN 에 대한 일부 또는 전체 정보를 얻는 것을 말한다. [3]

따라서, 스마트 TV 사용시 안전한 PIN 입력을 위해서는 엿보기 공격을 방지하면서 TV 의 제한적인 입력 방식을 고려한 적합한 PIN 입력 방식에 대한 연구가 필요하다. 특히 더이상 숫자 키에 대한 지속성이 없어진 배경으로 D-pad 를 활용한 사용자 인증 방식의 필요성이 대두된다. 이런 PIN 입력과 관련하여 Binary 방식, LIN 방식, Color PIN 방식 등 다양한 방식이 연구되어왔지만 이러한 방식들은 안전성 혹은 편의성에 있어서 문제를 가지고 있다.[4][5] 특히 리모컨을 사용하여 PIN 을 입력해야 하는 TV 환경에는 적합하지 않다.

그러므로 본 연구는 리모컨의 사 방향 키에 이를 누르는 압력 값을 적용한 사용자 인증 방식에 대한 엿보기 공격 보안성을 확인해 보고자 한다. 사 방향 키는 4 개의 키를 가지고 있기 때문에 전체 경우의 수가 256 가지밖에 없기 때문에 엿보기 공격에 의해 쉽게 노출 될 수 있다. 그렇기 때문에 이 방식에 대해 보안을 위한 추가적인 방식이 필요하고 이를 버튼 압력 값으로 확인해 보고자 한다. 이전 연구에 따르면 압력 힘을 이용한 보안 방식은 엿보기 공격에 상당히 보안성이 상승되고 있음을 보여주고 있고 [3][6] 사용자 인증 방식은 사용자가 사용하기 쉽게 구성되어야 하기 때문에 [7] 누르는 행위 이외에 추가적인 다른 행위를 추가 하지 않은 자연스러운 인증 방식이 될 수 있기 때문이다.

2. 실험 및 결과

본 연구의 실험은 총 2 파트로 이루어져 있다. 첫번째 실험은 파일럿으로 아이폰의 포스 터치 기술을 활용하여 총 28 명의 참여자에게 엿보기 공격 테스트를 진행하여 압력 값을 이용한 사용자 인증 방식이 엿보기 공격에 얼마나 강력한지 실험해 보았다. 두번째 실험은 실제 TV 리모컨을 활용하여 동일한 엿보기 공격 테스트를 진행하고 이를 분석해 보았다.

2.1 아이폰 포스 터치를 활용한 실험

첫번째 실험은 리모컨 키와 유사한 형태의 앱을 개발하여 엿보기 공격에 대해서 시뮬레이션 해보고 압력 값을 활용한 인증의 보안성에 대해서 간단하게 테스트를 해 보았다. 실험에 사용된 장비는 IPhone 6s 이며 해당 앱은 숫자, 4 방향, 압력이 추가된 4 방향 이렇게 3 가지 방식을 포함하고 있다. 이 때 압력 4 방향의 압력 값은 강하게/약하게 2 가지로만 구분하였고 아이폰의 최대 압력 값인 0.337N 의 75%인 0.25N 을 기준으로 이보다 강하면 “강”입력, 약하면 “약”입력으로 구분하게 하였다.

실험 참여는 총 28 명이 진행하였고 참가자는 가장 먼저 엿보기 공격 실험(Shoulder Surfing Attack Test, SSA Test)에 참여하였다. SSA Test 는 실험 진행자가 주어진 패드를 이용하여 숫자(Number PIN, NUM), 4 방향(Direction PIN, DP), 누르는 세기를 조정한 4 방향(Direction PIN with Pressure, DPP)의 3 가지 PIN 방식으로 자연스럽게 입력하면, 그것을 훔쳐보고 유추하는 실험으로 구성된다. 해당 실험 절차는 다음과 같다. 실험 참여자와 진행자에게 동일한 아이폰 세트가 주어지고 진행자는 미리 숙지한 입력 값을 실험 참여자가 잘 볼 수 있는 위치에서 입력한다. 이때 실험 참여자는 어느 위치에서도 자유롭게 훔쳐보는 것이 가능하고 진행자가 입력한 패스워드를 본인의 앱에 입력한다. 각 3 가지 방식당 5 번의 비밀번호가 주어지고 모든 참가자는 동일한 입력 세트를 사용한 과제를 수행하였다.

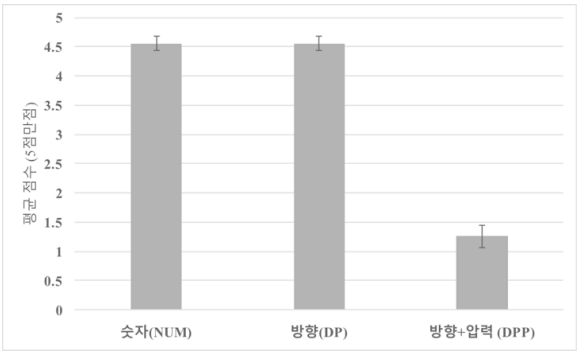

그림 1 아이폰을 활용한 SSA 테스트 결과

실험 1 의 결과는 압력을 추가한 4 방향 방식(M=1.26, SD=1.26)이 숫자(M=4.56, SD=0.64)와 4 방향 방식(M=4.56, SD=0.64)과 비교하여 점수가 낮았고 이는 단순하게 압력을 추가하는 것만으로도 엿보기 공격에 대한 보안성이 높아짐을 의미한다고 볼 수 있다.

2.2 두 개의 압력 값을 활용한 리모컨 인증 보안성

두번째 실험은 실제 리모컨과 압력 센서를 활용하여 압력의 보안성 확인을 진행하였다. 총 36 명의 참가자(나이 M=24.86 , SD =3.17)가 참여하였고 참가자는 이번에는 TV 리모컨을 사용하여 실험 1 과 동일한 SSA 테스트를 진행하였고 실험 진행자가 압력 센서가 장착된 리모컨으로 PIN 을 입력하면 참가자는 이를 훔쳐보고 동일한 리모컨을 받아 어떤 키를 눌렀는지 다시 입력하는 방식으로 진행하였다. 실험은 총 2 세트를 진행하였고 세트 별로 다른 실험자가 진행하되 순서는 무선화 하였다. 한 세트는 각 PIN 타입 별(NUM, DP, DPP)로 5 가지 종류의 4 자리 PIN 을 사용하였고, 해당 PIN 은 모든 참가자가 동일한 것으로 진행하였다. 실험 참가자는 위치와 상관없이 어떤 방식으로든 실험자의 리모컨을 관찰할 수 있게 하였다. 압력센서의 값으로 3kg 이상의 값을 강으로 인식하게끔 보정하고 실험을 진행하였다.

먼저 Shoulder Surfing 실험 결과는 각 PIN 타입별 10 번 시행 중 맞춘 횟수를 확인해 본 결과 [그림 2]와 같이 나왔다 Number PIN(M=6.25, SD=2.02), Direction PIN(M=7.92, SD=1.78), Direction PIN with pressure(M=3.69, SD=1.63). 이를 ANOVA 로 분석해 보면 비밀번호 타입 별 점수의 구형성 검정 결과, Mauchly 의 구형성 가정을 충족하였다(W=.85, p=.06). 또한 비밀번호 타입 간에 차이는 유의했다(F=71.96, MSE=158.37, p=.001, $\eta 2$=.67). Bonfferoni 사후 검증으로 NUM vs DP (p<.001), NUM vs DPP(p=.001), DP vs DPP(p=.001) 간의 차이가 모두 통계적으로 유의함을 확인했다. 즉, Direction PIN 방식은 기존 방식이라 할 수 있는 Number PIN 보다도 Shoulder Surfing 에 취약하지만 Direction PIN 에 Pressure 를 추가한 방식은 Number PIN 보다 보안 정도가 많이 개선되는 것을 확인할 수 있었다.

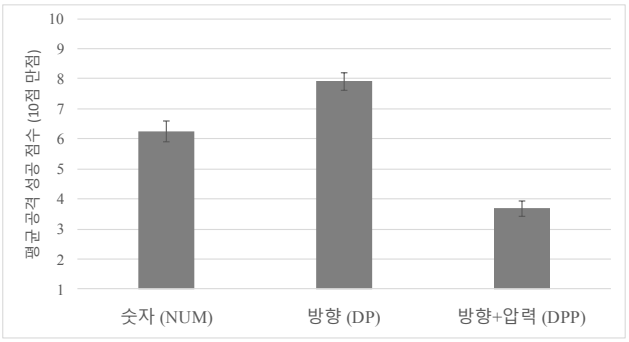

그림 2 리모컨을 활용한 SSA 테스트 결과

추가 분석으로 사용자의 비밀번호가 실제 비밀번호와 얼마나 유사한 지 판단하기 위해 각 PIN 타입 별 평균 Levenshtein distance 값을 알아보았다. Levenshtein distance 는 사용자 입력이 정답과 같아지기 위해 최소 몇개의 삽입, 삭제, 교체를 수행해야 하는지 알아보는 것으로 패스워드의 일치 비율을 측정하는데 많이 사용되는 알고리듬이다.[8] 이 실험의 경우 4 자리 모두 동일하면 distance 값은 0 이고 모두 불일치 하면 4 가 나온다.그 결과는 [그림 3]에서 볼 수 있는데 앞의 실험 결과와 동일하게 DPP 가 보안성에 가장 좋은 것으로 나왔다.

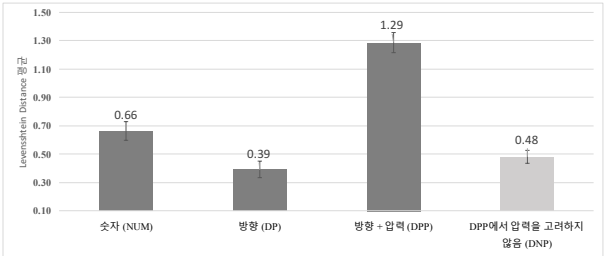

그림 3. Levenshtein Distance 결과 비교

이 결과에 대해서 확률적으로 이야기 해보면 4 자리 입력은 단순하게 수치적으로 보면 10 개의 키를 가지고 있는 Number PIN 에 대해서는 1/10000 이고 Direction PIN 은 1/256, Direction PIN with Pressure 는 1/4096 이기 때문에 Number PIN 이 가장 좋은 보안 정도를 가진다고 할 수 있다. 그러나 Distance 의 값을 보면 NUM 과 DP 방식은 확률적 값과 동일한 보안 순서를 가진다고 볼 수 있지만 DPP 는 다른 2 개에 비해 월등히 높고 이는 단순 확률로 수치적으로 계산되는 것보다 훨씬 높다는 것을 의미할 수 있다. 이 때 디스턴스 DPP 에서 압력

값을 고려하지 않고 방향만 확인한 디스턴스 값(DNP)은 0.48(SD=0.28)로 디스턴스 DP 의 값 (M=0.39, SD=0.36)과 통계적으로 차이가 없는 것으로 나타났다(p=.09). 이 결과는 보안성에 대해 방향에 대해서는 DP 와 동일한 보안 정도를 가지지만 여기에 압력만 더한 것으로 0.81 의 Distance 차이를 불러왔다

3. 결론

본 연구를 통해 앞으로 가전에서 사용될 Simple 리모컨에 적용될 수 있는 Direction PIN 방식은 기존의 Number PIN 방식에 비해 보안성이 매우 취약하다고 볼 수 있지만, 여기에 간단한 압력의 2 가지 레벨만 추가 하더라도 Shoulder Surfing Attack 같은 기본적인 해킹 방식에 대해서 보안성이 향상되는 것을 확인하였다. 또한 사용자 편의성에도 큰 문제가 없고 인증을 위한 사용자의 추가적인 행위를 요구하지 않기 때문에 편리한 인증 방식이 될 가능성이 있다. 그러므로 압력을 추가한 리모컨은 4 방향키만 사용하기 때문에 사용자의 입력 편의성을 유지하면서도, 보안성을 높일 수 있는 방식으로 다양한 제품과 스마트 디바이스에 활용될 수 있을 것이다.

사사의 글

본 과제(결과물)는 서울시 지원으로 수행한 「서울시 창조전문 인력양성사업(CAC15113)」의 결과입니다.

참고 문헌

1. Kassim, M. M. and Sujitha, A. (2013), ProcurePass: A User Authentication Protocol to Resist Password Stealing and Password Reuse Attack, Computational and Business Intelligence (ISCBI), 2013 International Symposium on. IEEE, 31-34.
2. Mun-Kyu Lee, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry", *IEEE Transaction*, vol. 09, no. 3, pp. 631-645, April 2014.
3. Luo JN., Yang MH., Tsai CL. (2016) A Mobile Device-Based Antishoulder-Surfing Identity Authentication Mechanism. In: Chen J., Piuri V., Su C., Yung M. (eds) Network and System Security. NSS 2016. Lecture Notes in Computer Science, vol 9955. Springer, Cham
4. Golle, P., & Wagner, D. (2007, May). Cryptanalysis of a cognitive authentication scheme. In Security and Privacy, 2007. SP'07. IEEE Symposium on (pp. 66-70). IEEE.
5. 신동오, 강전일, 맹영재 & 양대헌. (2009, 12) "S3PAS의 교치 공격에 대한 취약성 분석 . 한국정보보호학회 동계학술대회 논문집, 19(2). pp. 409
6. Malek, B., Orozco, M., & El Saddik, A. (2006, July). Novel shoulder-surfing resistant haptic-based graphical password. In Proc. EuroHaptics (Vol. 6)
7. Kim, C. S., & Lee, M. K. (2010, January). Secure and user friendly PIN entry method. In Consumer Electronics (ICCE), 2010 Digest of Technical Papers International Conference on (pp. 203-204). IEEE.
8. V. I. Levenshtein. Binary codes capable of correcting deletions, insertions and reversals. Soviet Physics Doklady, 10(8):707－710, 1966.