Journal of Korea Multimedia Society Vol. 24, No. 3, March 2021(pp. 440-447)
https://doi.org/10.9717/kmms.2020.24.3.440

폴더블 스크린 기반 기기 사용자 인증기법 연구

최 동 민†

A Study on User Authentication Method for Foldable Screen-Based Devices

Dongmin Choi†

ABSTRACT

Smartphones are currently being produced with similar functions, shapes, and software. The foldable smartphone is a product that dramatically changed the shape of the existing smartphone. Therefore, it affects the functions and software. In this paper, we analyze the potential security vulnerability of current mobile authentication methods by dividing them into two parts, security vulnerabilities of non-foldable smartphones, and security vulnerability that appears with the changed smartphone structure. According to the analysis result, the classic and current mobile user authentication methods appears to be easily affected by the smartphone display structure. Finally, we propose an appropriate authentication method as well as the concept of security measures for smartphones with foldable screen. Our method shows that it is more secure than the conventional authentication methods in foldable display smartphone.

Key words: Foldable Screen, Authentication Method, In-folding Structure

1. 서 론

최근 고정형 바타입 일변도의 스마트폰 제품 시장에서 물리 폼팩터 한계를 벗어나려는 다양한 시도가 감지되고 있으며 일부는 2019년 하반기부터 완성품으로 시장에 출시되었다. 현재 시장에 공급되고 있는 대표적 사례는 플렉서블 디스플레이를 도입한 폴더블 스마트폰이다[1-4]. 폴더블 스마트폰은 휘어지는 디스플레이가 장착된 스마트폰을 통칭하며[5,6] 기존과는 차별화된 구조 및 동작을 갖는다. 여기에는 삼성의 갤럭시Z 시리즈[1], 모토로라의 RAZR[2], Royole의 FlexPai 시리즈[3], 화웨이의 Mate Xs[4] 등이 있으며, 폴더블 스마트폰의 판매량은 2019년에 100만대, 이후 2025년에는 1억대로 급성장할 것으로 예측된다. 이에 주요 스마트폰 생산 기업들도 폴더블 스마트폰에 주력하는 것으로 알려져 있고[7-9] 이는 스마트폰 폼팩터의 지속적인 변화가 있을 것을 의미한다. 하드웨어의 구조적 변화는 전용 소프트웨어에 영향을 미치므로 변형 폼팩터의 핵심 요소인 폴더블 디스플레이 역시 기존 보안체계에 어느 정도 영향을 줄 것으로 예상할 수 있다. 본 연구는 현재 초기 변형 폼팩터 및 폼리스 스마트폰 시장의 주력 모델인 폴더블 스마트폰에 적용된 고전 사용자 인증 기법의 보안 취약점과 안전성을 기존 고정형 바 타입 모양의 범용 스마트폰과 비교 분석하며, 발생 가능한 공격의 유형을 언급하고 이에 대응이 가능한 폴더블 스마트폰에 적합한 사용자 인증 기법을 제안한다.

본 연구는 다음과 같이 구성된다. 2장에서 우리는 기존의 고전 사용자 인증 기법을 포함하여 몇 가지 대표적인 인증 기법들의 보안 대책과 앞으로 발생하

※ Corresponding Author : Dongmin Choi, Address: (61452) Pilmun-daero, Dong-gu, Gwangju, Korea, TEL : +82-62-230-7996, FAX : +82-, E-mail : jdmcc@chosun.ac.kr
Receipt date : Feb. 20, 2021, Revision date : Mar. 13, 2021
Approval date : Mar. 15, 2021
† Div. of Undeclared Majors, Chosun University
※ This research was supported by research fund from Chosun University(2020).

게 될 취약점들에 대해 분석하며 이에 대한 보안 대책을 언급한다. 3장에서는 이러한 유형의 보안 취약점에 대응하는 인증 기법을 제안하고 기법의 동작 구조를 설명한다. 4장에서는 폴더블 스마트폰 사용 환경에서 제안 기법을 기존 기법과 보안 안전성 및 사용 편의성 측면에서 비교하며 5장에서 결론을 맺는다.

2. 관련 연구

스마트폰 사용자 인증 기법은 2007년 LG의 터치스크린 기반 스마트폰의 출시[10] 이래 지금까지 거의 유사한 형태의 고정형 바 타입 스마트폰에 내장되어 사용되고 있으며 그 종류는 텍스트 및 그래픽 정보 기반 패스워드, 패턴, PIN, OTP, 지문, 음성, 서명, 홍채, 얼굴, 행위, 키스트로크 감지와 같은 기법들로 구분되어 사용되고 있다. 본 장에서는 이러한 기법 중 폴더블 디스플레이의 물리적 특성과 연관이 있고 보편적으로 사용되는 기법인 PIN[11]과 패턴[12] 기법에서 발생 가능한 보안 취약점을 보인다.

2.1 고전 보안 위협 모델과 기존 인증 기법

고전 보안 위협 모델

- 무차별 대입(Brute force) 공격[13]과 사전 공격[14]의 두 가지 방식은 모두 원사용자의 정상적인 아이디와 패스워드를 추측하여 시도하는 방식의 공격 기법이다. 무차별 대입 공격의 경우 공격자가 사용 가능한 모든 가용 비밀키 조합을 입력하여 맞는 비밀키를 발견하기까지 공격을 시도하는 매우 단순한 위협 모델이다. 이 방식은 비밀키의 길이에 공격 성공률과 성공에 소비되는 시간이 의존적이며 공격자는 비밀키 입력에 대한 경우의 수를 설정할 수 있는 거의 모든 방식의 보안 기법에 대해 이와 같은 공격을 시도할 수 있다. 사전 공격의 경우 무차별 대입 공격과 달리 비밀키가 의미 있는 문자 집합일 경우에 더 무게를 둔 공격 기법으로 사용자의 비밀키가 사용자에게 있어 특정한 의미가 있는 문자 집합일 것으로 가정하고 이를 사전의 문자 집합과 대조하여 맞는 비밀키를 발견하기까지 공격을 시도하는 위협 모델이다. 이 방식은 주로 텍스트 기반 비밀정보에 대해 유효하며 비밀키가 의미 있는 문자 집합일 경우 무차별 대입 공격보다 공격 성공률이 높으며 소비시간도 더욱 줄어든다.

기존 인증 기법

- PIN 기법은 기본적인 스마트폰 사용자 인증 기법으로 이외에도 인터넷뱅킹이나 신용카드 인증 또는 도어락 시스템에도 사용되는 범용성이 높은 사용자 인증 기법이다. 이 기법은 4~8자리 정도의 숫자를 비밀키로 사용하는 입력의 편의성과 아울러 숫자 범위의 한계성으로 인해 고전 보안 위협에 매우 취약한 인증 기법이다.

- 패턴 기법의 경우 9개의 점을 기준으로 사용자가 지정한 임의의 선분 조합 패턴을 비밀키로 사용하는 인증 기법이다. 이 기법은 터치스크린 입력의 편리함과 신속함으로 인해 보편적으로 사용되고 있으며 문자에 기반한 고전 보안 위협에 대해 PIN 기법보다 안전하다고 할 수 있다.

2.2 폴더블 디스플레이 특성과 잠재적 보안 위협 모델

폴더블 디스플레이 특성

- 폴더블 디스플레이는 최대 180도까지 휘어짐이 가능한 소재로 만든 플렉서블 디스플레이를 의미한다. 폴더블 디스플레이를 적용한 스마트폰은 Fig. 1과 같이 크게 인 폴딩과 아웃 폴딩 방식으로 구분되며 디스플레이 개수 및 위치에 따라 세부적으로 분류된다[5].

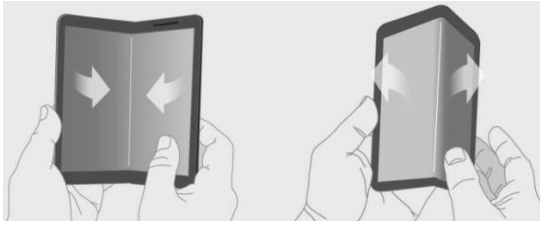


Fig. 1. In-folding and out-folding display [15].

폴더블 디스플레이가 적용된 스마트폰은 Fig. 2와 같이 크기 변형에 따른 소형화, 그리고 화면 확장에 따른 정보표시량 증가와 같은 장점이 있어 새로운 방식의 응용이 가능하나 비밀정보의 표시 및 입력 면에서 볼 때 더욱 높은 보안상 취약점을 갖게 될 수 있다. 예를 들어 아웃 폴딩 구조의 경우 스마트폰 외부 스크린 구조로 인해 의도치 않은 비밀정보의 누설이 가능하며 인 폴딩 구조의 경우 접는 각도에

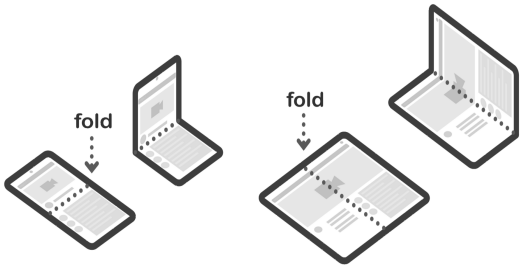


Fig. 2. Different types of single screen-based foldable [6].

따라 비밀정보를 유출하게 될 수 있다.

잠재적 보안 위협 모델

- 사회공학 공격[16] 중 엿보기 공격[17,18]은 비밀정보를 취득하기 위해 정상 사용자의 어깨너머로 공격자가 비밀정보를 직접 눈으로 보고 취득하는 공격으로 하드웨어 또는 소프트웨어의 취약점 대신 사용자 부주의를 이용한다는 점에서 기존의 고전 보안 위협과는 궤를 달리하는 공격 기법이다. 모바일 기기를 이용한 개인정보 또는 금융정보와 같은 치명적인 정보를 처리하는 비중이 높아져 감에 따라 보안정책 개선, 전용 인증 기법 개발 및 제고가 이루어지고 있으나 이를 취급하는 사용자에 의해 발생하는 부주의와 같은 문제는 언제나 발생할 수 있으며, 모바일 기기를 이용하는 장소는 대개 타인의 접근이 쉬운 공용 장소이므로 사용자 부주의를 이용한 공격은 매우 효과적이다.

- 레코딩 공격[19]의 기본개념은 엿보기 공격과 같으나 사용하는 도구에 차이가 있다. 엿보기 공격은 직접적인 관찰로 정보를 획득하는 기법이며 레코딩 공격은 다양한 종류의 광학 영상기록장치와 같은 장비를 사용하여 정보를 획득하므로 엿보기 공격에 비하면 취득 영상의 반복재생이나 확대 기능을 이용할 수 있어 공격 성공률이 높다. 엿보기 공격이나 레코딩 공격 모두 단일 공격자를 기준으로 가정하고 있으나 다수의 공격자[20]를 고려한다면 더욱 높은 공격 성공률을 보일 것으로 예상할 수 있다.

- 스머지 공격[21]은 스마트폰 화면에 표시된 비밀정보를 손가락으로 터치할 때 묻은 유분 흔적을 복원, 비밀정보를 추정 및 조합하여 탈취하는 공격으로 화면의 비밀정보 입력 위치에 변화가 없는 기법은 모두 이 공격에 취약하다.

- 열 감지 공격[22]은 화면의 비밀정보를 손가락으로 터치한 후 일정 시간 화면에 남아있는 손가락 체열 흔적을 열 감지 카메라를 이용해 복원, 비밀정보를 추정 및 조합하여 탈취하는 공격으로써 스머지 공격과 감지 대상 및 복원 기술을 제외한 모든 부분이 유사하므로 스머지 공격에 취약한 보안 기법 모두 열 감지 공격에 취약하다. 이 공격도 저가격, 고성능의 열화상 카메라 내장 스마트폰[23] 및 스마트폰용 열화상 카메라 모듈[24] 등을 사용할 수 있어 비교적 쉽게 비밀정보 유출이 가능하다.

2.3 보안 위협 대응 고려사항

무차별 대입 및 사전 공격 대응

- 확률 선택에 의한 무차별 대입 및 사전 공격은 경우의 수를 증가시켜 시간을 지연시키는 방안과 확률요소가 개입되기 어려운 비밀정보를 사용하는 방법으로 분류하여 대응할 수 있다. 예를 들어 경우의 수를 증가시키는 경우 비밀정보 입력에 사용되는 문자, 그래픽 또는 패턴의 후보집단을 증가시킬 수 있다. 다른 방식으로 비밀정보에 해당하는 문자, 그래픽 또는 패턴의 길이와 복잡도를 늘려 공격을 지연시킬 수 있으며 확률요소가 개입되기 어려운 생체정보를 사용하여 대응할 수 있다.

잠재적 보안 위협 대응

- 엿보기, 레코딩, 스머지, 열 감지 공격은 인적 오류에 기반한 사회공학 기법으로 보안 기법을 사용하는 사용자와 보안 기법 사이에서 발생하는 취약점에 집중하는 공격이므로 보안 알고리즘의 암호학적 안전성 이외에도 보안 기법과 사용자 사이의 사용자 인터페이스 부분에서부터 보안 기법의 기기 환경까지 모두 고려해야 한다. 사용자 인터페이스 부분은 사용자와 보안 알고리즘 사이에 비밀정보를 입력하고 입력받는 중요한 요소이며 사회공학 공격은 주로 이 부분에서 발생하는 인적 오류에 주목하여 공격을 시도하므로 사용자 인터페이스를 통한 비밀정보의 입력이 스크린에 표시되지 않도록 하거나 표시되더라도 추정이 어렵게 하는 방법으로 대응할 수 있다. 기기 환경에 대한 고려는 해당 보안 기법이 동작하는 스마트폰 폼팩터 특히, 디스플레이 크기 또는 기기의 구조가 주로 이에 해당하며 예를 들어 폴더블 디스플레이를 사용하는 스마트폰의 경우 접었을 때와 펼쳤을 때의 디스플레이 면적이 2배 정도 차이가 있다는

점을 고려한다면 스마트폰 화면을 펼쳤을 때 엿보기 공격이나 레코딩 공격에 더욱 취약할 수 있음을 알 수 있다. 따라서 기기 환경에 대한 고려가 포함되어야 효과적으로 대응할 수 있다.

3. 제 안

앞서 언급한 대응 고려사항을 만족하기 위해 다음과 같이 발전된 형태의 PIN 사용자 인증 방식을 제안한다. 제안하는 방식은 간접 키 입력 기법[25]보다 간단한 키 입력 구조를 보이며 보안 위협 대응 고려사항에서 언급한 확률요소, 사용자 인터페이스의 보안성, 그리고 기기 환경을 고려하였다.

3.1 구조

제안하는 기법의 사용자 인터페이스에 해당하는 화면 표시부 및 입력 구조는 Fig. 3과 같다.

Fig. 3의 (a)는 해당 기법에서 사용하는 전체 키 풀을 의미한다. 풀의 크기는 최대 n x m(키 풀 문자 집합의 행과 열) 크기로 확장 가능하며 키 풀에 사용되는 문자도 숫자, 알파벳 및 특수문자를 적용할 수 있고 모든 문자의 배치는 임의배치이다. 이렇게 표시된 키 풀 구조는 Fig. 3의 (3) touch and swipe와 같이 스와이프 기능을 이용해 상하좌우로 이동 가능하며 순환식 테이블 구조를 갖추고 있다. 예를 들어 (1) 상단의 '0 1 2 3 4 5 6'의 경우 화면 임의 위치에서 위로 한번 스와이프하면 (1)의 하단부에 있는 '9 0 1 2 3 4 5' 자리에 '0 1 2 3 4 5 6'이 이동하며 원래 '0 1 2 3 4 5 6' 자리에는 아래 행의 '7 8 9 0 1 2 3'이 순차적으로 이동한다. (3) touch and swipe의 아래 또는 좌우 스와이프의 경우에도 각각의 방향에 따라 순환하여 키 풀의 행과 열이 순차적으로 이동하는

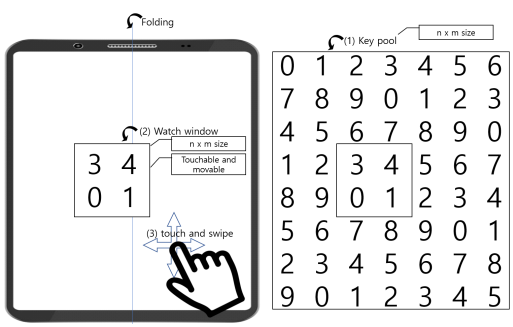


Fig. 3. User interface of proposed method.

구조이다. (2) watch window는 사용자가 문자를 보기 위한 정보 표시창으로 키 풀의 정보를 오직 이 창을 통해서만 볼 수 있고 이 창 이외의 위치는 모두 가려져 있어 볼 수 없는 구조를 갖는다. 또한 (2) watch window는 n × m 크기를 갖는 가변형으로 사용자에 의해 크기가 정의되며 위치도 자유롭게 이동할 수 있으므로 폴더블 스마트폰의 경우 스마트폰 화면상 임의의 위치에 이 창을 이동시켜놓아 발생 가능한 사회공학 공격 시도에도 어느 정도 물리적 대응이 가능하다. 다음의 Fig. 4의 (a) 및 (b)는 watch window 크기와 위치 변화에 대한 예시이다.

3.2 키 설정

보관용 패스워드 생성은 기존의 PIN 기법과 같이 4~8자리의 숫자 또는 문자 평문 텍스트 형태로 입력을 받으며 숫자 입력을 기준으로 한다. 이 패스워드는 인증 서버에 저장되어 값의 유출을 방지하며 키 풀의 크기 및 사용되는 문자의 종류는 최대 n × m 크기 내에서 사용자에 의해 결정된다. 키 풀의 크기는 최소 3 × 3에서부터 n × m 크기로, 화면 표시 문자의 크기와 종류도 같이 결정된다. 이후 watch window의 크기를 결정하는데 이 크기는 2 × 2에서 키

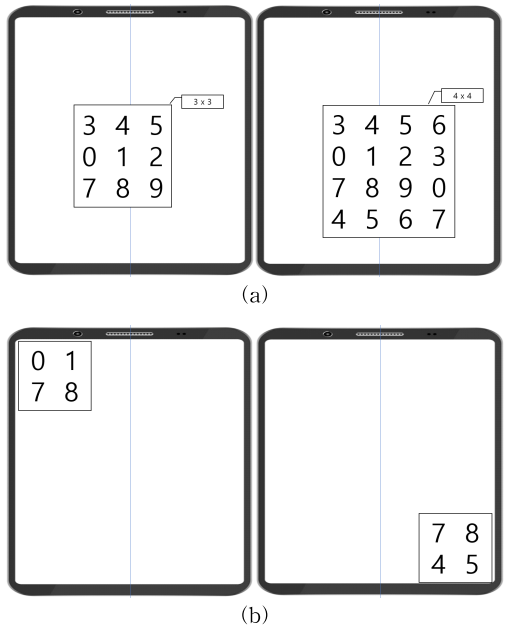


Fig. 4. Functions of watch window. (a) variable size and (b) location.

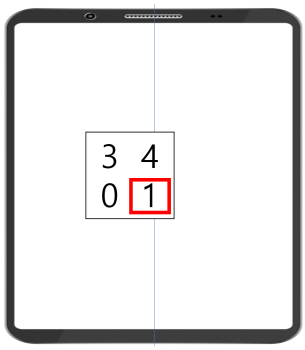


Fig. 5. Location pointer in watch window.

풀의 최대크기인 n × m까지 설정 가능하며 위치 포인터로 사용될 행렬 좌표 역시 설정 단계에서 사용자가 결정한다.

Fig. 5의 붉은 사각형은 위치 포인터를 의미하며 이 표시는 실제로는 보이지 않는다. 여기서는 (2, 2) 위치 즉, 2행 2열이 위치 포인터가 되어 이 위치의 값이 실제 입력되는 값이다.

3.3 사용자 인증

Fig. 6은 키 설정 단계에서 설정된 패스워드 값이 '1234', 8 × 7의 키 풀 크기, 2 × 2의 watch window, (2, 2)의 위치 포인터로 설정한 상태의 패스워드 입력에 대한 예시이다. 현재 watch window의 (2, 2)에 '1' 이 있으므로 그대로 Fig 6. 의 (1) 터치 동작과 같이 스크린 아무 곳이나 터치하여 '1'을 입력한다. 이후, 상하좌우로 스와이프하다 보면 '2'를 찾게 되며 '2'를 watch window의 (2, 2) 자리에 맞추어 놓고 스크린 아무 곳이나 터치하여 '2'를 입력한다.

Fig. 6에서는 바로 옆자리에 '2'가 있는 것으로 설정했으므로 왼쪽으로 한번 (2) 스와이프하여 '2'를 watch window의 (2, 2) 자리에 맞춘 후 (3) 터치하는 것으로 '2'를 입력한다. 그다음 (4) 스와이프 동작으로 '3'을 찾고 (5) 터치하여 '3'을 입력하며, 이후 (6) 스와이프, (7) 터치 동작으로 '4'를 입력한다. Fig. 6에서는 왼쪽 스와이프 동작만 계속 발생하였으나 실제 환경에서는 숫자를 찾기 위해 (2), (4), (6) 각각의 동작에 여러 방향 및 횟수의 스와이프 과정이 추가될 수 있다.

Table 1. Security countermeasure comparison (C: Considered, N: Not considered).

Type of Attack	Authentication Method		
	PIN	Pattern	Proposed
Brute Force	C	C	C
Dictionary	C	C	C
Shoulder Surfing	N	N	C
Recording	N	N	C
Smudge	N	N	C
Thermal	N	N	C

4. 보안성 검토

제안 기법은 간접 키 입력 기법으로 고전 PIN 입력과 전혀 다른 방식으로 동작한다. 제안 기법은 패스워드 입력에 가상 키패드를 이용하거나 직접 입력을 사용하지 않아 키 입력이 유출되지 않는다. 제안 기법은 화면상의 watch window에 표시된 정보만을 이용하여 스와이프 및 터치의 두 가지 동작만으로 조작하여 입력할 수 있어 동작이 간편하고 입력 오류가 낮다. 우리는 제안 기법을 본문에서 언급한 고전 및 사회공학 공격들에 대해 기존의 유명 인증기법인 PIN, 패턴 인증기법들과 안전성 면에서 비교하였다. 다음의 Table 1은 기존의 PIN, 패턴 기법과 제안 기법을 고전 및 사회공학 공격에 대해 해당 공격에 대

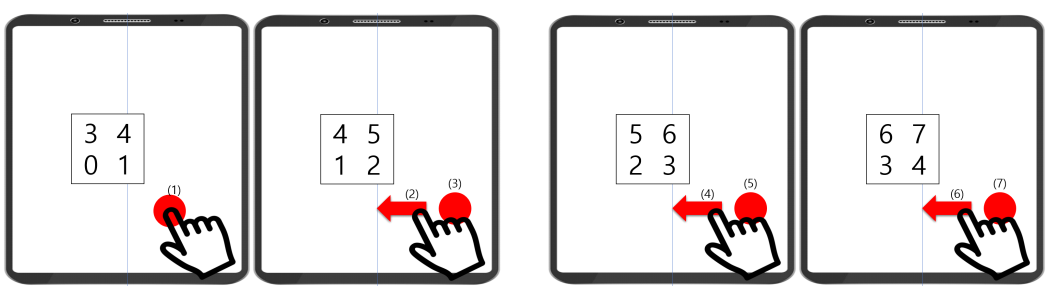


Fig. 6. Procedure for entering password '1234'.

한 고려가 있는지를 비교한 안전성 비교표이다.

PIN과 패턴 인증기법의 경우 무차별 대입 및 사전 공격에 대해 입력횟수 제한 등과 같은 대응이 가능하며 패스워드 및 패턴 길이 조절로 안전성 향상이 가능하나 PIN의 비밀문자 집합은 0~9의 범위에 자릿수의 제약이 있고 사회공학 공격에 대한 고려가 없다. 엿보기 공격 및 레코딩 공격에 대해 PIN 및 패턴 기법은 터치스크린의 가상 키패드에 대한 손가락 터치 동작이 그대로 노출된다. 스머지와 열 감지 공격의 경우에도 해당 PIN 및 패턴 기법의 사용자 인터페이스에 변수가 없다면 유분 및 잔열을 감지한 후 바로 공격을 시도할 수 있어 취약하다고 할 수 있다.

제안 기법의 경우, 고전 공격 기법에 대한 대응으로 PIN과 유사한 패스워드 길이 조절 방식이 사용될 수 있으며 비밀문자 집합은 숫자 이외에도 문자 및 도형이나 기호도 사용 가능하므로 확률적 안전성이 PIN에 비해 높다. 엿보기 및 레코딩 공격에 대해 제안 기법은 터치스크린의 가상 키패드에 대한 손가락 터치 동작이 PIN, 패턴 기법과 같이 공격자에게 노출되지만 노출되는 정보의 경우의 수가 password 각각의 자리에 대해 최소 2×2에서 최대 $m \times n$이 되며, 노출된다고 하더라도 입력정보가 바로 유출되지 않는다. 스머지와 열 감지 공격의 경우 제안 기법은 화면에 표시된 사용자 인터페이스 구성이 임의 변경되므로 유분 및 잔열을 감지하더라도 패스워드 복원이 어려워 바로 공격을 시도할 수 없다.

5. 결 론

본 연구에서 우리는 새로운 스마트폰 폼팩터에 따른 기존 보안 기법의 안전성 검토와 아울러 고전 및 최근 공격 유형에 대응하기 위한 고려사항을 언급하고 이를 만족하는 기법을 제안하였다. 새로운 스마트폰 물리 규격은 이를 바탕으로 하는 전용 소프트웨어에 영향을 주며 보안 기법 역시 영향을 받게 되므로 대응이 필요하다. 제안하는 기법은 기존의 PIN 및 패턴 기법에서 발생하게 되는 보안상 취약점을 고려하였고 편의성을 저해하지 않는 방향으로 사용자 인터페이스가 구성되었으며 패스워드 입력 방법도 PIN의 가상키보드 입력 방법 대비 단순 스와이프 및 터치의 두 가지 동작으로만 패스워드 입력이 가능하도록 구성되었다. 제안 기법은 PIN, 패턴 기법 대비 전사 공격에 확률적 안전성이 높으며 사회공학 공격에 패스워드의 직접 유출이 어려우나 여전히 패턴 기법에 비해서는 낮은 사용자 편의성을 갖고 있으므로 연구가 필요하다. 이에 우리는 향후 연구로써 제안 기법의 문자기반 입력 대신 그래픽, 패턴, 이미지의 형태를 고려한 사용자 인증기법을 고안하고 입력을 더욱 단순화시켜 사용자 편의성을 높이고자 한다.

REFERENCE

[1] Samsung Galaxy fold 5G(2019). https://www.samsung.com/sec/smartphones/galaxy-fold-sm-f907/SM-F907NZSAKOO/ (accessed February 19, 2021).

[2] Motorola razr(2020). https://www.motorola.co.uk/smartphones-razr (accessed February 19, 2021).

[3] Royole FlexPai 2 5G(2020). https://global.royole.com/en/flexpai (accessed February 19, 2021).

[4] Huawei Mate Xs 5G(2019). https://consumer.huawei.com/kr/phones/mate-x-s/ (accessed February 19, 2021).

[5] Tech yourself Foldable Phones in 10 steps: Report(2018). https://www.slashgear.com/samsung-galaxy-foldable-smartphone-details-analysis-industry-market-14557949/ (accessed February 19, 2021).

[6] Folding the Web Enabling real responsive design on foldable devices(2020). https://medium.com/samsung-internet-dev/folding-the-web-90952c925d52 (accessed February 19, 2021).

[7] Foldables to Hit 100 Million by 2025(2020). https://www.strategyanalytics.com/access-services/devices/mobile-phones/emerging-device-technologies/reports/report-detail/foldables-to-hit-100-million-by-2025 (accessed February 19, 2021).

[8] Samsung Electronics earnings outlook: Promoting popularization of foldable smartphones next year(2020). http://www.thelec.kr/news/articleView.html?idxno=8543 (accessed February 19, 2021).

[9] iPhone Flip: Everything we know about Apple's foldable phone plans(2021). https://www.to

msguide.com/news/iphone-flip-everything-we-know-about-apples-foldable-phone-plans (accessed February 20, 2021).

[10] From the 'Brick' to New Foldable Phones: The History of the Mobile Form Factor(2020). https://community.arm.com/developer/ip-products/processors/b/processors-ip-blog/posts/history-of-the-mobile-form-factor (accessed February 20, 2021).

[11] J. Bonneau, S. Preibusch, and R. Anderson, "A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs," *Proceeding of International Conference on Financial Cryptography and Data Security*, pp. 25-40, 2012.

[12] M. Shahzad, A. X. Liu, and A. Samuel, "Secure unlocking of mobile touch screen devices by simple gestures: You can see it but you can not do it," *Proceeding of the 19th Annual International Conference on Mobile Computing & Networking*, pp. 39, 2013.

[13] I. Kim, "Keypad against Brute Force Attacks on Smartphones," *IET Information Security*, Vol. 6, No. 2, pp. 71-76, 2012.

[14] A.K. Kyaw, F. Sioquim, and J. Joseph, "Dictionary Attack on Wordpress: Security and Forensic Analysis," *Proceedings of the 2nd International Conference on Information Security and Cyber Forensics*, pp. 158-164, 2015.

[15] Samsung picks in-folding type for foldable smartphone(2017). http://www.theinvestor.co.kr/view.php?ud=20170928000900 (accessed February 20, 2021).

[16] Social Engineering Attacks: Common Techniques & How to Prevent an Attack(2020). https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack (accessed February 20, 2021).

[17] E. Miluzzo, A. Varshavsky, S. Balakrishnan, and R.R. Choudhury, "TapPrints: Your Finger Taps Have Fingerprints," *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*, pp. 323-336, 2012.

[18] H. Kim, H. Seo, Y. Lee, T. Park, and H. Kim, "Implementation of Secure Virtual Financial Keypad for Shoulder Surfing Attack," *Korea Institute of Information Security and Cryptography*, Vol. 23, No. 6, pp. 21-29, 2013.

[19] T. Takada, "Fake Pointer: An Authentication Scheme for Improving Security against Peeping Attacks using Video Cameras," *Proceeding of International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, pp. 395-400, 2008.

[20] X. Su ,Z. Wang, X. Liu, C. Choi, and D. Choi, "Study to Improve Security for IoT Smart Device Controller: Drawbacks and Counter-measures," *Security and Communication Networks*, Vol. 2018, No. 4296934, pp. 1-14, 2018.

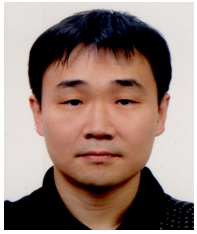
[21] A.J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J.M. Smith, "Smudge Attacks on Smartphone Touch Screens," *Proceeding of USENIX Conference on Offensive Technologies*, pp. 1-7, 2010.

[22] Y. Abdelrahman, M. Khamis, S. Schneegass, and F. Alt, "Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication," *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pp. 3751 - 3763, 2017.

[23] Integrated thermal imaging(2019). https://www.catphones.com/en-dk/features/integrated-thermal-imaging/ (accessed February 19, 2021).

[24] FLIR ONE PRO LT(2020). https://www.flirkorea.com/products/flir-one-pro-lt/ (accessed February 20, 2021).

[25] D. Choi, "Indirect PIN Entry Method for Mobile Banking Using Relative Location Information of Secret Code," *Journal of Korea Multimedia Society*, Vol. 23, No. 6, pp. 738-746, 2020.



최 동 민

2003년 2월 경희대학교 공과대학 졸업(공학사)
2007년 7월 조선대학교 교육대학원 졸업(교육학석사)
2011년 2월 조선대학교 일반대학원 컴퓨터공학과(공학박사)

2011년~2013년 조선대학교 BK사업팀 연구교수
2014년~현재 조선대학교 자유전공학부 부교수
관심분야 : 정보 보안, 정보 윤리, 애드혹 네트워크, 센서 네트워크 보안, 모바일 보안