Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.4, Aug. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.4.903

기계 학습 기반의 자동화된 스머지 공격과 패턴 락 시스템 안전성 분석*

정 성 미,† 권 태 경‡
연세대학교 정보보호연구실

Automated Smudge Attacks Based on Machine Learning and Security Analysis of Pattern Lock Systems*

Sungmi Jung,† Taekyoung Kwon‡
Information Security Lab., Graduate school of Information, Yonsei University

요 약

터치스크린 기반 스마트 기기가 널리 보급 되면서 모바일 환경을 위한 주요 인증 메커니즘으로 그래픽 패스워드 기법 중 하나인 패턴 락 시스템이 등장했다. 사용자가 잠금 해제를 위하여 패턴 락을 사용한 후의 남아있는 패턴 모양의 흔적은 스머지 공격에 취약하다. 이러한 스머지 공격에 대응하기 위하여 TinyLock을 포함한 다양한 패턴 락이 제안되었다. 본 논문에서는 스머지 공격이 발생할 수 있는 환경에서 획득한 스머지 패턴 이미지를 이용하여 기계 학습을 통한 자동화된 스머지 공격의 유효성에 대하여 실험하고 안드로이드 패턴 락과 TinyLock의 안전성에 대하여 비교 분석하였다. 자동화된 스머지 공격에서 높은 공격 성공률을 보였으며 기존에 많이 사용되고 있는 안드로이드 패턴 락이 TinyLock보다 더 안전하지 않음을 검증하였다.

ABSTRACT

As smart mobile devices having touchscreens are growingly deployed, a pattern lock system, which is one of the graphical password systems, has become a major authentication mechanism. However, a user's unlocking behaviour leaves smudges on a touchscreen and they are vulnerable to the so-called smudge attacks. Smudges can help an adversary guess a secret pattern correctly. Several advanced pattern lock systems, such as TinyLock, have been developed to resist the smudge attacks. In this paper, we study an automated smudge attack that employs machine learning techniques and its effectiveness in comparison to the human-only smudge attacks. We also compare Android pattern lock and TinyLock schemes in terms of security. Our study shows that the automated smudge attacks are significantly advanced to the human-only attacks with regard to a success ratio, and though the TinyLock system is more secure than the Android pattern lock system.

Keywords: Smartphone, Pattern Lock System, Machine Learning, Smudge Attack

Received(03. 16. 2016), Modified(07. 07. 2016), Accepted(07. 28. 2016)

* 본 논문은 2015년도 동계 학술대회에 발표한 우수논문을 개선 및 확장한 것임.

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2016-H8501-16-1008). 또한, 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2015R1A2A2A01004792).

† 주저자, sm.jung@yonsei.ac.kr

‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

I. 서 론

최근 터치스크린 패널이 탑재된 스마트 기기의 사용이 급격히 증가하면서 사용자들은 손가락을 이용하여 이메일, 소셜 네트워크 서비스, 스마트폰 결제 등의 다양한 스마트 기기의 기능들을 이용하게 되었다. 특히 사생활 침해 방지를 위하여 PIN, 패스워드와 같은 스마트폰 잠금장치를 사용하는데 사용자들은 기억하기 쉬운 텍스트 기반의 패스워드를 선택하기 때문에 공격자 또한 쉽게 추측할 수 있다. 기존의 PIN, 패스워드를 대체할 수 있는 다양한 그래픽 패스워드(Graphical password) 스킴들이 꾸준히 제안되어 왔다[9][10][13]. 안전성과 사용성이 균형을 이루는 것은 여전히 문제이나 사람이 단어보다 그래픽 정보를 기억하는 것에 더 적합하기 때문에[1] 그래픽 패스워드를 사용하는 것이 유용하다.

안드로이드 패턴 락 시스템은 Draw-A-Secret (DAS)[11] 스킴에 기반하여 2008년 구글 안드로이드에 도입된 패턴 기반의 그래픽 패스워드 잠금 기법이다. 패턴 락은 3x3의 작은 점으로 구성되어 있으며 세 가지 규칙에 의해 비밀 패턴을 설정하여 사용할 수 있다. 최소 4개 이상의 포인트의 연결로 이루어져야 하며 각각의 포인트는 한 번씩만 사용되어야 한다. 그리고 2개의 포인트 사이에 존재하는 포인트는 건너뛰지 않고 반드시 포함되어야 한다. 이러한 규칙을 지키면서 사용할 수 있는 패턴의 종류는 389,112개가 존재한다[4]. 그 중 사용자들은 기억하기 쉽고 그리기 쉬운 패턴을 주로 사용하기 때문에 추측 공격이 쉬울 수 있다[2].

사용자가 스마트 기기를 사용하기 위하여 디스플레이를 터치할 경우 터치스크린에 흔적, 즉 스머지(Smudges 또는 Oily residues)가 남게 된다(Fig. 1.). 이 스머지는 최근에 사용했거나 자주 사용하는 터치 위치를 짐작할 수 있도록 하며, 이를 통해 공격자는 사용자가 사용하는 모바일 패턴 락의 형태를 추측하여 공격하는 것이 가능해진다. 이를 스머지 공격(Smudge Attacks)이라고 한다. 2010년 Aviv는 안드로이드 패턴 락에 대한 스머지 공격을 처음으로 제안하였으며, 스머지는 끊임없이 발생하고 쉽게 지워지지 않으며 카메라와 같은 장비로 수집 및 분석이 가능하기 때문에 스머지 공격의 위험성이 존재한다고 언급하였다[4]. 이러한 스머지 공격에 대응하기 위하여 2014년 Tinylock 인증 기법이 제안되었으며 높은 안전성이 검증되었다. Ⅱ장 관련 연구에서 더 자세하게 언급하도록 하겠다.

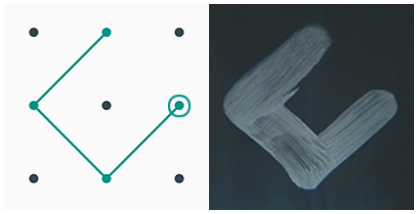


Fig. 1. Smudge in smartphone touchscreen

본 논문에서는 카메라로 캡쳐한 스머지 패턴 이미지를 이용하여 기계 학습 기반의 자동화된 스머지 공격의 유효성에 대하여 실험하며 안드로이드 패턴 락 인증 기법의 안전성을 검증하고자 한다. 본 논문의 순서로는 Ⅱ장에서 기존 스머지 공격에 대한 선행 연구들에 대하여 정리하며 Ⅲ장에서 기계 학습을 통한 자동화된 스머지 공격에 대하여 살펴보며 Ⅳ장에서는 연구 방법에 대하여 설명한다. Ⅴ장에서는 실험 결과에 대하여 언급하고 마지막으로 Ⅵ장을 통해 이 논문의 결론을 짓는다.

II. 관련 연구

Aviv 등은 안드로이드 패턴 락에 대한 스머지 공격을 처음으로 구체적인 실험을 통해 제안하였으며, 스머지가 쉽게 노출될 수 있는 환경을 조사하고 가장 이상적인 환경에서 발생할 수 있는 스마트폰 스머지 공격의 가능성을 실험하였다. 화면 터치, 애플리케이션 사용, 스크린 표면에 얼굴이 닿는 등 실제 스마트폰 사용 후 이루어진 패턴 입력이 오히려 터치스크린의 노폐물 위에 남겨진 스머지로 인하여 더 명확한 추측이 가능함도 보였다[4]. 한편 Andriotis 등은 전처리 과정(Image processing)과 신경망

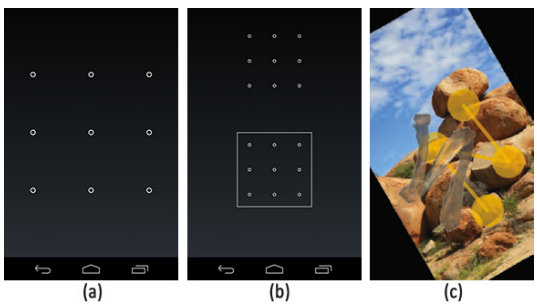


Fig. 2. Pattern Lock System (a) Android Pattern Lock (b) TinyLock[12] (c) SmudgeSafe[14]

(Neural network)을 이용하여 스머지 패턴 공격을 위한 프로세스를 제안[3]하였지만, 구체적인 실험 방법과 결과에 대한 언급은 하지 않았다.

스마트폰 환경에서의 스머지 공격에 안전한 패턴 락 인증 기법을 제안한 연구들이 있다. Kwon 등은 스머지를 통한 추측 공격을 방지하기 위하여 TinyLock 인증 기법을 제안하였다. 기존의 패턴 락 보다 작은 화면에서 인증 패턴을 입력한 뒤 가상 휠 입력 단계를 거쳐 남아있는 스머지 정보를 자연스럽게 지울 수 있다. 사용자들을 대상으로 스머지 패턴 사진을 이용한 비밀번호 패턴 유추 실험을 하여 안전성을 검증하였고, 세 번에 걸쳐 TinyLock을 사용함으로써 사용성 검증을 하였다. 기존 패턴 락 보다 사용 속도는 조금 느리지만 스머지 공격에 대하여 안전하다는 결과를 보였다[12]. Schneegass 등은 이미지 이동, 확대/축소, 회전, 자르기, 반전 등의 이미지의 변형을 통해 스머지 공격에 대응하는 SmudgeSafe 인증 기법을 제안하였다. 기존의 PIN, 안드로이드 패턴 락 시스템과의 안전성을 비교 분석한 결과 역시 더 안전하다는 결과를 보였다[14]. von Zezschwitz 등은 4가지의 패턴 락을 제안하였다. 사용자 실험, 설문조사를 통해 4가지 패턴 락의 안전성, 사용성에 대하여 비교 분석하였다[17].

III. 기계 학습 기반의 스머지 공격

본 연구에서는 기계 학습 기반의 자동화된 스머지 공격의 유효성과 그 결과에 대해서 조명해본다. 스머지 공격을 언급한 선행 연구들은 사람이 육안으로 스머지를 보고 추측 공격을 하였지만 자동화된 스머지 공격에서는 기계 학습 알고리즘을 통해 스머지 이미지를 미리 학습시키고 예측하는 공격을 수행한다. 이를 위해 적절한 스머지 패턴들을 수집하고 가장 적합한 기계 학습 알고리즘을 찾아내어 분석하는 것이 필요하다.

따라서 OpenCV 라이브러리를 통한 전처리 과정(Image processing)을 거친 후 스머지 패턴 분석 및 스머지 공격에 대한 유효성을 실험하기 위해 패턴 인식 분야에서 가장 많이 활용되고 이미지 분류에 효율적인 기계 학습 중 하나인 k-최근접 이웃(k-NN, k-Nearest Neighbor) 알고리즘을 선택하였다.

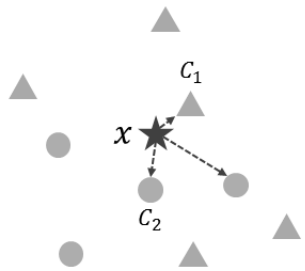


Fig. 3. Classification of the object (x) in k-NN

3.1 k-최근접 이웃 분류

k-NN이란 입력된 객체에 가까운 k개의 근접 이웃들의 과반수 의결에 의해서 클래스를 결정해주는 알고리즘[8]으로 유클리드 거리 측정법[7]을 사용하여 주로 패턴 인식에서 활용되고 있다. 또한 구현이 간단하며 데이터가 많을수록 일관성 있는 결과를 도출해내는 장점이 있다.

k-NN은 k값에 따라 결과가 다르게 나타날 수 있어[6] 가장 적합한 k값을 결정하는 것이 중요하다. 예를 들어, Fig. 3.에서 입력된 객체 x를 클래스로 할당한다고 할 때 k=1일 경우에는 C_1으로 분류될 것이고, k=3일 경우에는 C_2로 분류될 것이다.

IV. 연구 방법

스머지 패턴 분석을 위해 현재 모바일에서 사용되고 있는 기본 안드로이드 패턴 락 인증 기법과 패턴 입력 후 가상 휠을 통해 스머지를 지우는 효과를 보여주는 스머지 공격에 안전한 TinyLock[12] 인증 기법을 대상으로 실험한다.

4.1 연구 설계

본 연구에서는 세 가지 상태에 따른 안드로이드 패턴 락과 TinyLock의 자동화된 스머지 공격의 유효성을 실험하기 위하여 패턴의 상태 간에는 between-group, 패턴 락 시스템 간에는 within-group 실험을 진행하였으므로 split-plot study를 설계하였다. 개체 내 검정에 사용된 변수(within-subjects variables)는 패턴 락 시스템(안드로이드 패턴 락, TinyLock)이고, 개체 간 검정에 사용된 변수(between-subjects factors)는 패턴의 상태(Clean, Dots, Keypad)이다. 패턴의 상태는 다양한

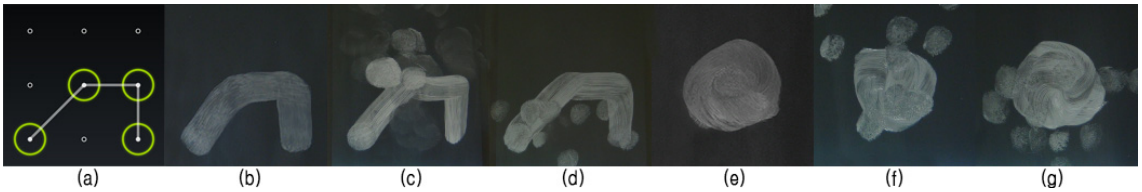


Fig. 4. Smudges (a) Real pattern (b) Clean smudge in Android Pattern Lock (c) Dots smudge in Android Pattern Lock (d) Keypad smudge in Android Pattern Lock (e) Clean smudge in TinyLock (f) Dots smudge in TinyLock (g) Keypad smudge in TinyLock

환경에서 발생할 수 있는 스머지를 세 가지 상태로 구분하였다. 패턴 락을 사용한 후에 어떠한 행동도 하지 않은 깨끗한 패턴(Clean), 패턴 입력 후 지하철 어플리케이션을 사용한 단순 터치 패턴(Dots), 패턴 입력 후 SMS 문자 기능을 이용한 키패드 사용 패턴(Keypad)을 고려하였다. Fig. 4.는 패턴의 세 가지 상태에 따른 안드로이드 패턴 락과 TinyLock 각각의 스머지를 촬영하여 비교한 것이다.

4.1.1 패턴 템플릿 선정

기존의 선행 연구들은 사용자들로부터 안드로이드 패턴 락 시스템에서 자주 사용하는 패턴들을 수집하여 패턴들의 특징을 언급하고 있다. 주로 왼쪽 방향에서 오른쪽 방향으로의 패턴 그리기를 선호하였으며 평균 길이 6이하의 패턴들로 구성되어 있었다[5][15][16].

본 실험을 수행하기 위해 선행 연구 결과들을 고려하여 패턴 템플릿을 선정하였다. 점 4~5개를 경유하며 평균 길이 5 이하로 구성된 단순한 패턴(Simple pattern)과 점 7~9개를 경유하며 평균 길이 6 이상으로 구성된 복잡한 패턴(Complex pattern)을 균등하게 구성하였으며, 각각 100개씩 총 200개의 랜덤 패턴을 선택하였다.

4.1.2 데이터 수집

스머지 촬영을 위하여 약 두 달간 사용자가 직접 안드로이드 패턴 락과 TinyLock을 사용하였으며, 터치스크린에 남은 스머지 이미지 촬영을 통해 총 3,200개(각각 150x150 pixel)의 데이터를 수집하였다. 훈련 데이터, 테스트 데이터는 각각 2,000개, 1,200개를 사용하였으며 테스트 데이터는 Clean, Dots, Keypad로 구분하여 각각 400개씩 사용하였다.

4.2 실험 환경

자동화된 스머지 공격에 대한 패턴 락의 안전성 분석을 위한 실험 환경은 Table 1.과 같다.

Table 1. Experiment environment

Capture Photo	Galaxy Nexus, Sony HDR-PJ580
Develop Environment	Python 2.7, Numpy 1.8.0
Library	OpenCV 2.4.11
Machine Learning	k-NN
Spec	Intel Core i5 CPU 2.60GHz, 8.00GB, 64bits

4.3 실험 대상

패턴 수집을 위한 스머지 이미지 촬영에 총 6명(남자 3명, 여자 3명)이 실험에 참여하였다. 참가자들의 나이는 27~30세(평균 28.5세)의 대학원생을 대상으로 하였으며 패턴 락 시스템을 사용해 본 익숙한 사용자들로 구성하였다.

4.4 실험 절차

수집한 데이터를 바탕으로 안드로이드 패턴 락과 TinyLock 각각 동일한 절차로 수행하였으며 실험 절차는 Fig. 5.와 같다. 이 때 데이터로 사용되는 모든 스머지 이미지는 cvtColor 알고리즘을 통해 RGB 모드에서 Gray 모드로 변환되고, 임계값을 65로 설정한 이진화(Threshold) 처리를 통해 전처리 단계를 거친다. 전처리 단계를 수행한 각각의 템플릿에 대하여 Label을 생성하고 훈련 데이터를 기계학습(k-NN) 알고리즘을 통해 트레이닝 시킨 후 예

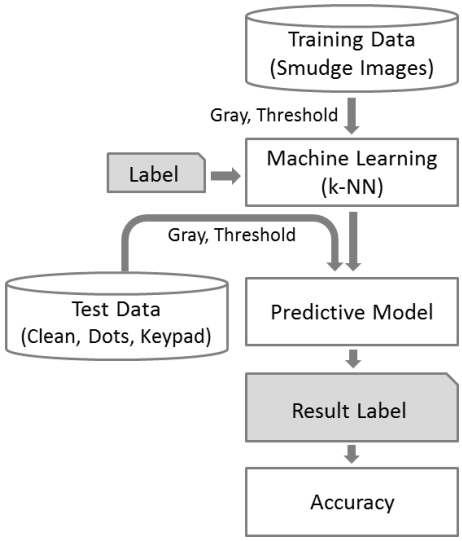


Fig. 5. Experiment procedure

측 모델을 생성한다. 생성된 예측 모델을 기반으로 입력된 각각의 패턴 상태 별 테스트 데이터에 대해 추측한 결과 Label 값과 이전에 생성한 훈련 데이터의 Label 값을 비교하여 매칭 여부를 판단하고 정확도를 계산한다.

4.5 연구 가설

본 연구에서는 연구 질문을 TinyLock이 안드로이드 패턴 락보다 더 안전한가? 패턴의 상태에 따라 공격률의 차이가 있는가?로 설정하였으며 이에 따라 다음과 같은 가설을 세웠다.

- H1: TinyLock은 안드로이드 패턴 락보다 자동화된 스머지 공격에 더 안전하다.
- H2: 패턴의 상태에 따른 스머지 공격률은 유사하다.

Table 2. Results of automated smudge attack (mean)

State	Pattern Lock(%)	TinyLock(%)
Clean	97.5	2
Dots	90	1
Keypad	89.5	0.5
Mean	92.33	1.17

V. 실험 결과

안드로이드 스머지 패턴 공격 실험 결과는 패턴 락 시스템, 패턴의 상태, 패턴의 강도 별로 구분하여 Fig. 6.에서 보여주고 있으며 Table 2.에서는 평균 공격 성공률에 대하여 요약하였다. 선행 연구들과 패턴 템플릿의 유사성이 높다고 가정할 때 기존 안드로이드 패턴 락은 평균적으로 92% 이상의 높은 매칭률을 보였는데 이는 사람에 의한 안드로이드 패턴 락 공격 성공률(68%)[4]과 큰 차이를 보인다. 또한 TinyLock은 평균 2% 미만의 매우 낮은 매칭률을 보여 사람에 의한 TinyLock 공격률(0%)[12]과 큰 차이는 없었지만 공격 성공률이 조금 높아진 결과를 보였다.

기계 학습 인식 결과 정확도는 안드로이드 패턴 락과 TinyLock 모두 Clean, Dots, Keypad 순으로 높게 나타났고 패턴 락 사용 후 어떤 행동도 하

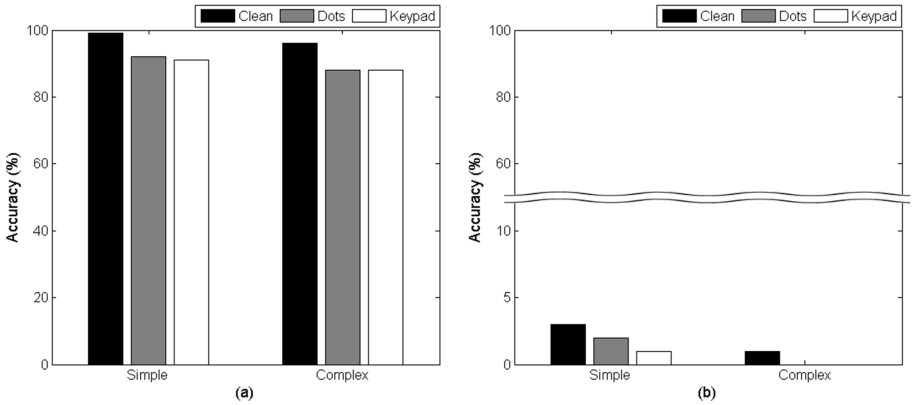


Fig. 6. Smudge Pattern Analysis. (a) Android Pattern Lock (b) TinyLock

지 않은 경우(Clean)에 각각 평균 97.5%, 2%로 패턴 유추 가능성이 가장 높았다. 또한 복잡한(Complex) 패턴보다 단순한(Simple) 패턴이 더 높은 정확도를 보여 사용자들이 많이 선택하는 단순한 패턴이 스머지 공격에 더 취약함을 알 수 있었다. TinyLock의 경우 100개 중 3개 이하의 확률로 스머지 유추 공격에 성공한다는 것을 뜻한다. TinyLock은 가상 휠 단계를 통해 입력한 패턴의 모양이 지워지게 됨으로써 비밀 패턴의 모양을 구분하기 어렵기 때문에 기존의 안드로이드 패턴 락보다 스머지 공격에 대하여 더 안전하다고 할 수 있다.

5.1 가설 검정

Table 3.은 4.5절에서 제시한 가설을 검정하기 위하여 사용한 개체 간 요인, 개체 내 변수명(2열)과 검정 결과를 요약하여 보여준다.

패턴 락 시스템 간에 차이를 평가하기 위하여 일반 선형 모형의 반복 측정 ANOVA로 분석한 결과 개체 내(within-subjects) 효과 검정으로부터 패턴 락 시스템(안드로이드 패턴 락, TinyLock) 간에는 유의한 차이가 있음을 검정하였다($p \leq 0.001$). 즉 안드로이드 패턴 락은 자동화된 스머지 공격에 매우 취약한 반면 TinyLock은 자동화된 스머지 공격에 매우 안전하다는 것을 알 수 있었다. 이를 통해 가설 1은 채택되었다.

스머지 패턴 상태 간의 차이를 평가하기 위하여 동일한 측정 방법으로 분석한 결과 개체 간(between-subjects) 효과 검정으로부터 패턴의 상태(Clean, Dots, Keypad) 간의 차이는 유의하지 않다고 나타났다($p \geq 0.05$). 이는 안드로이드 패턴 락과 TinyLock 각각에 대하여 스머지의 상태에 따른 자동화된 스머지 공격률은 서로 유사하다고 볼 수 있으며 패턴의 상태에 상관없이 자동화된 스머지 공격에서 안드로이드 패턴 락은 높은 공격률로 유사하며 TinyLock은 낮은 공격률로 유사하다는 것을 알 수 있다. 이를 통해 가설 2는 채택되었다.

Table 3. Results of hypothesis test (* within subjects variables, ** between subjects factors)

Hypo-thesis	Independent Variables	F	p-value	Result
H1	Pattern Lock*	32520.111	.000	accept
H2	State**	1.681	.324	accept

VI. 결 론

본 논문에서는 터치스크린 기반 스마트 기기에서 발생할 수 있는 자동화된 스머지 공격의 유효성을 기계 학습을 이용하여 분석하였다. TinyLock 인증 기법은 매칭률이 낮아 기존의 결과와 비교하여도 스머지 공격에 여전히 안전한 반면 현재 많이 사용되고 있는 안드로이드 패턴 락의 경우 모든 경우에서 매칭률이 높았으며 기존의 사람 공격 결과와 큰 차이를 보여 스머지 패턴 유추 공격에 매우 취약하다는 것을 검증할 수 있었다. 더불어 스머지 패턴들의 상태는 공격 성공률에 영향을 미치지 않았다.

자동화된 스머지 공격 결과를 통해 향후에는 더욱 안전하고 사용성이 높은 패턴 락 인증 기법이 필요함을 알 수 있었다. 최근 패턴 인증이 결제 수단으로도 사용되고 있는 만큼 스머지 공격으로부터 안전한 시스템이 활용되어야 할 것이며 이는 TinyLock 인증 기법으로 대체가 가능할 것으로 보인다.

6.1 한계점 및 향후 연구

본 연구의 한계점은 389,112개의 넓은 패턴 공간에서 패턴을 대규모로 수집하는 데에 시간적인 제약이 있었기 때문에 200개의 패턴 템플릿만을 적용하였다는 점이다. 패턴 템플릿의 종류를 더욱 다양하게 구성한 큰 규모의 후속 연구도 가능할 것이다. 더불어 SmudgeSafe 인증 기법을 대상으로 자동화된 스머지 공격을 적용해 볼 수 있을 것이며 새로운 패턴 락 시스템의 설계도 필요할 것이다.

또 다른 한계점은 실험에 사용된 테스트 데이터의 세 가지 상태에 대한 것이다. 본 연구에서는 스머지가 잘 노출될 수 있는 깨끗한 화면에서 패턴 락 시스템을 사용 후 지하철 어플리케이션을 사용하거나 문자 기능을 이용하였는데, 비밀 패턴을 그릴 때의 손가락의 압력보다 어플리케이션을 사용할 때의 압력이 낮았기 때문에 비교적 비밀 패턴의 흔적이 식별 가능한 정도로 남아있었다. 보다 더 보편적인 스마트폰 사용 환경에서의 패턴의 상태들을 고려한 연구가 필요할 것으로 보인다.

향후 연구에서는 본 연구의 k-NN 알고리즘만을 사용한 스머지 패턴 분석을 다른 기계 학습 알고리즘의 적용으로 확장하여 더 보편적이고 다양한 환경에서 발생할 수 있는 스머지 상태에 따른 자동화된 스

머지 공격과 이것을 바탕으로 한 추측 공격의 능력에 대하여 더욱 면밀히 분석할 것이다.

References

[1] A. De. Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, Vol. 63, no. 1, pp. 128 - 152, July 2005.

[2] P. Andriotis, T. Tryfonas, G. Oikonomou, and C. Yildiz, "A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks," In Proc. of the sixth ACM conference on Security and privacy in wireless and mobile networks (WiSec'13), pp. 1-6, April 2013.

[3] P. Andriotis, T. Tryfonas, and Z. Yu, "POSTER: Breaking the Android Pattern Lock Screen with Neural Networks and Smudge Attacks," In Proc. of the sixth ACM conference on Security and privacy in wireless and mobile networks (WiSec'14), July 2014.

[4] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge Attacks on Smartphone Touch Screens," In Proc. of the 4th USENIX Conference on Offensive Technologies (WOOT'10), pp. 1-7, Aug. 2010.

[5] A. J. Aviv, D. Budzitowski, and R. Kuber, "Is Bigger Better? Comparing User-Generated Passwords on 3x3 vs. 4x4 Grid Sizes for Android's Pattern Unlock," In Proc. of the 31st Annual Computer Security Applications Conference (ACSAC' 16), pp. 301-310, Dec. 2015.

[6] C. M. Bishop, Pattern Recognition and Machine Learning, Springer, Aug. 2006.

[7] P. E. Danielsson, "Euclidean Distance Mapping," Computer Graphics and image processing, Elsevier, Vol. 14, no. 3, pp. 227-248, Nov. 1980.

[8] B. V. Dasarathy, Nearest Neighbor (NN) Norms: NN Pattern Classification Techniques, IEEE Computer Society Press, 1991.

[9] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," In USENIX Security Symposium, Aug. 2004.

[10] H. Gao, X. Guo, X. Chen, L.Wang, and X. Liu, "Yagp: Yet another graphical password strategy," Annual Computer Security Applications Conference (ACSAC'08), pp. 121 - 129, Dec. 2008.

[11] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," In Proc. of the 8th Conference on USENIX Security Symposium (SSYM'99), pp. 1-14, Aug. 1999.

[12] T. Kwon, and S. Na, "TinyLock: Affordable Defense Against Smudge Attacks on Smartphone Pattern Lock Systems," Computers & Security, Elsevier, Vol. 42, pp. 137-150, May 2014.

[13] K. Renaud and A. D. Angeli, "Visual passwords: Cure-all or snake-oil?," Communications of the ACM, Vol. 52, no. 12, pp. 135 - 140, Dec. 2009.

[14] S. Schneegass, F. Steimle, A. Bulling, F. Alt, and A. Schmidt, "Smudgesafe: Geometric Image Transformations for Smudge-Resistant User Authentication," In Proc. of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp'14), pp. 775-786, Sep. 2014.

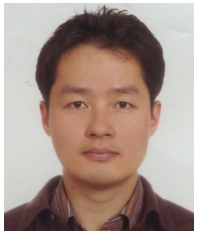
[15] Y. Song, G. Cho, S. Oh, H. Kim, and J. H. Huh, "On the effectiveness of pattern lock strength meters: Measuring the strength of real world pattern locks," In Proc. of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI'15), pp. 2343-2352, April 2015.

〔16〕 S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz, "Quantifying the security of graphical passwords: The case of Android unlock patterns," In Proc. of the 2013 ACM SIGSAC conference on Computer \& communications security (CCS'13), pp. 161-172, Nov. 2013.

〔17〕 E. v. Zezschwitz, A. Koslow, A. De Luca, and H. Hussmann, "Making Graphic-Based Authentication Secure Against Smudge Attacks," In Proc. of the International Conference on Intelligent User Interfaces (IUI'13), pp. 277-286, March 2013.

〈저자소개〉

정 성 미 (Sungmi Jung) 학생회원
2012년 2월: 강남대학교 미디어정보공학, 컴퓨터공학 학사
2013년 9월~현재: 연세대학교 정보대학원 석사과정
〈관심분야〉 Usable Security, Machine Learning 등



권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년~2000년: U.C. Berkely Post-Doc.
2001년~2013년 8월: 세종대학교 컴퓨터공학과 교수
2007년~2008년: Univ. Maryland at College Park 교환교수
2013년 9월~현재: 연세대학교 정보대학원 교수
〈관심분야〉 암호 프로토콜, 네트워크 프로토콜, IoT 보안, Usable Security, HCI 등