Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.5, Oct. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.5.1113

스머지 기반의 스마트 기기 지문 인증 공격 연구*

김 승 연,† 구 예 은, 권 태 경‡
연세대학교 정보보호연구실

Smudge-Based Smart Device Fingerprint Authentication Attack Study*

Seungyeon Kim,† Yeeun Ku, Taekyoung Kwon‡
Information Security Lab., Graduation School of Information, Yonsei University

요 약

스마트 기기에서 지문 인증은 가장 널리 쓰이는 생체 인증 방식이지만 스마트 기기의 특성에 의해 위조 지문에 취약하다. 본 논문에서는 먼저 기기 사용 후 남은 지문 흔적인 스머지를 활용하여 정당한 사용자의 협조 없이 위조 지문을 만들고 실제 상용 스마트폰의 지문 인증 통과가 가능함을 검증하였다. 이러한 스머지 기반 공격을 방지하기 위한 기술적 대응 방법으로 터치 스크린 위에서 지문 인증을 수행하고 UI를 옆으로 끌어서 지문 흔적을 제거하는 방법인 under-screen Touch ID with slide bar가 제안된 바 있다. 본 논문에서는 앞서 제안한 공격 방법과 이에 대한 대응 방법에 관한 사용자 인식을 61명 규모 사용자 설문 연구를 통해 분석하였다.

ABSTRACT

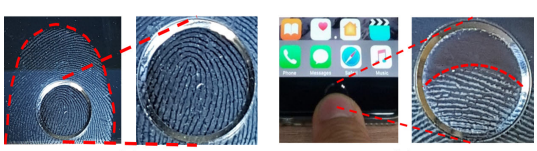
Fingerprint authentication is the most popular biometric in smart devices. However it has vulnerability to fake fingerprints. This paper shows that it is possible to pass fingerprint authentication of smartphone by creating counterfeit fingerprint without approval of legitimate users. As a technical countermeasure to prevent such a smudge-based attack, there has been proposed an under-screen Touch ID with a slide bar, which is a method of removing the fingerprint trail by dragging the UI to the side after fingerprint authentication on the touch screen. In this paper, we analyze how the proposed attack method and mitigation are perceived by actual user through 61 user survey.

Keywords: Smartphone, Fingerprint, Smudge, Authentication

I. 서 론

스마트폰, 태블릿 PC와 같은 휴대용 스마트 기기에서 지문 인증 기능은 그 편리함에 의해 널리 사용되고 있다. 세계 기술 산업 시장을 분석하는 업체 카운터포인트는 2018년에 출하되는 스마트폰의 71%에 지문 인증 기능이 탑재될 것으로 예상하였다[1].

그러나 현재 스마트폰에서 사용되는 지문 인증은 대체로 Fig.1-(1).과 같이 실제 지문에 비해 훨씬 작은 인식 센서를 사용한다. 이는 Fig.1-(2).와 같이 전체 센서를 사용하지 않고도 지문 인증을 통과 가능하다는 점과 결합되어 매우 작은 넓이의 지문을



(1) (2)

Fig. 1. Small Fingerprint Sensor

Received(07. 16. 2018), Accepted(08. 14. 2018)
* 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원(No.2017-0-00380, 차세대 인증 기술 개발)과 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 지원을 받아 수행된 연구임(IITP-2018-2016-0-00304).
† 주저자, tribunus000@yonsei.ac.kr
‡ 교신저자, taekyoung@yonsei.ac.kr(Corresponding author)

정교하게 위조할 수 있다면 공격자가 지문 인증을 통과할 수 있다는 점을 시사한다. 터치스크린을 사용하는 스마트 기기의 특성상 사용 흔적인 스머지(Smudge)가 남게 되며 스마트폰 조작에 주로 몇몇 손가락만 사용하는[2] 이러한 스머지로부터 지문 위조를 위한 단서를 발견할 가능성은 낮지 않다.

본 연구는 공격자가 스마트 기기의 터치스크린 표면에서 이러한 지문 스머지를 활용하여 실제 스마트 기기의 지문 인증 통과가 가능함을 보이고 사용자의 인식과 대조하여 실질적인 보안 위협임을 보인다. 또한 지문 인증의 취약점을 보완하는 방법을 소개하며 이에 대한 사용자 인식을 분석한다.

II. 배경 및 관련연구

Aviv 등은 안드로이드 패턴 락 인증을 공격하기 위해 터치스크린에 남은 스머지를 사진 촬영하여 활용하는 기법을 최초로 연구하였다[4]. Jung 등은 촬영된 패턴 스머지를 k-NN 기계학습 알고리즘으로 분석하여 패턴을 추측하는 자동화된 공격 방법의 유효성을 검증하였다[7]. Lee 등은 Aviv 등의 연구를 바탕으로 스머지를 사진 촬영하여 좋은 품질의 지문 이미지를 획득하는 방법인 SCRAP (Smudges Collected Reconstruction And sPoofing)을 제안했으며 개요는 다음과 같다[3].

1) 스머지 수집: 촬영환경을 구성하여 스마트폰 표면에서 스머지를 촬영 후 Watershed 알고리즘을 사용하여 터치스크린의 스머지 중 사용자 지문일 가능성이 있는 후보군을 추출한다. 추출된 후보군과 홈 버튼에 남아 있는 지문 스머지를 확대 촬영한다.

2) 매칭: 촬영된 이미지들을 흑백화 한 후 SIFT descriptor-based brute-force 매칭과 MINDTCT를 사용하여 홈 버튼에서 획득한 지문과 가장 유사도가 높은 터치스크린 지문 이미지를 선정하고 홈 버튼의 지문 이미지와 각도, 크기를 맞춘다.

3) 이미지 품질 평가: SIFT keypoints를 기준으로 두 이미지(홈 버튼의 이미지와 매칭 단계에서 최종 선정된 이미지)의 손상 정도를 식별한다. 두 이미지를 각각 10x10으로 분할한 후 영역 당 평균 키포인트 개수(τ)를 각 영역의 키포인트 개수와 비교하여 각 영역의 손상 여부를 판정한다. 손상 영역 수를 척도로 하는 비교 절차에 따라 두 이미지 중 더 좋은 품질을 가진 이미지를 선정한다.

4) 이미지 구성: 3)에서 산출된 결과에 따라 이 단계에서의 수행 작업이 달라진다. 터치스크린의 지문 이미지가 더 품질이 좋을 경우에는 특별한 추가 작업 없이 터치스크린의 지문 이미지를 최종 획득 이미지로 사용하며 그 반대의 경우에는 홈 버튼 지문 이미지의 손상된 영역을 터치스크린 지문 이미지의 같은 영역으로 대체하여 이를 최종 획득 이미지로 사용한다. 본 연구는 공격자가 Lee 등이 제안한 SCRAP 방법으로 좋은 품질의 지문 이미지를 획득하였다고 전제한다.

Cao 등은 전도성 인쇄물을 사용하여 지문 인증을 통과할 수 있음을 보였다[5]. 제조사 AgIC의 전도성 잉크 및 전도성 종이에 지문을 인쇄하여 실제 지문이 등록된 Samsung Galaxy S6와 Huawei Honor 7에 실제 지문처럼 사용이 가능함을 보였으며 이러한 방법은 기존에 널리 알려진 wood Glue를 사용한 위조 지문 방식에 비해 훨씬 빠르고 간편함을 보였다. 그러나 Cao 등이 제안한 방법은 공격이 아닌 위조에만 초점을 맞추고 있어 실제 지문 소유자의 직접적인 협조가 필요하다. 본 연구는 사용자의 직접적 협조 없이 SCRAP 방법으로 획득된 지문 이미지를 활용한 공격 방법을 보인다.

III. 제안하는 공격 및 대응 방법

3.1 공격자

본 연구에서 가정하는 공격자는 Lee 등의 연구[3]에서 가정한 공격자가 SCRAP을 성공적으로 수행한 경우이다. 즉, 공격자는 사용자의 스마트폰을 획득하였고 조명과 카메라를 자유로이 조정하여 사진 촬영할 수 있으며 이를 통해 빠른 시간 내에 지문 이미지를 획득한 사람이다. 빠른 시간이란 마지막 잠금 해제 이후 오랜 시간이 경과하지 않아 다시 지문 인증을 시도할 수 있을 정도의 시간을 의미한다. 예를 들어 iPhone의 경우 마지막 잠금 해제 이후 48시간이 경과하면 지문 인증으로 잠금 해제가 불가하다. Table 1.에 iPhone과 Galaxy의 최대 등록 가능한 지문 개수와 최대 시도 횟수, 마지막 잠금 해제 이후 지문 인증 가능한 경과 시간이 요약되어 있다.

3.2 공격 절차

3.1절에서 가정한 공격자는 인쇄 전에 추가적인 이미지 처리 과정이 필요하다. 절차는 다음과 같다.

1) Lee 등의 연구[3]에서는 지문 이미지들 간의 유사도를 측정하는 방식으로 실험을 수행하였으나 본 연구에서는 지문을 인쇄하고 실제 지문 인식 센서를 대상으로 하므로 좌우 반전한다.

2) 지문의 돌출된 부분이 흰색(스머지)으로 나타나 있으므로 흑백 반전한다.

3) 이미지(지문 융선)의 선명도를 높이기 위해 히스토그램 평활화 과정을 거친다. 선명도가 충분히 높다고 판단될 경우 이 과정을 생략할 수 있다.

4) 지문의 융선만 남기고 배경을 제거하기 위해 SourceAFIS[6]를 사용한다. SourceAFIS는 지문 이미지를 입력 받아 유사도를 출력하는 소프트웨어로 지문 이미지에 관한 다양한 기능을 제공한다.

위에서 기술한 이미지 변환 과정의 사례가 Fig.2.에 도시되어 있다. 최종 변환된 이미지를 Cao 등의 연구[5]를 참고하여 AgIC 전도성 잉크와 전도성 종이를 사용하여 인쇄한다. 인쇄 크기는 먼저 홈 버튼 지문 이미지를 홈 버튼 크기를 기준으로 크기 설정한 후 최종 변환 이미지와 홈 버튼 이미지의 융선 두께가 유사하도록 최종 변환 이미지의 크기를 변화시키며 설정한다. 지름 0.2mm 내외의 크기 오차는 허용된다. 인쇄에는 전도성 잉크 제조사 AgIC에서 권장하는 EPSON L361 프린터를 사용하였다.

3.3 실험

3.3.1 실험 설계

Fig.2.의 최종 변환 이미지를 인쇄한 위조 지문으로 3명의 참가자가 Galaxy S7, S8에 잠금 해제 5회씩을 시도하였다. 참가자 3명은 모두 스마트폰 지문 인식 사용 경험이 있으며 위조 지문으로 지문 인증 통과 경험은 없었다. 인증 시도는 각 잠금 해제마다 최대 5회씩 가능하였다. 이는 Table 1.에 나타난 바와 같이 실제 스마트폰에는 인증 시도가 가능한 횟수에 제한이 있다는 점을 반영한 것이다.

Table 1. Fingerprint authentication in smartphone

Device	iPhone 5S, 6S, 7, 7 Plus	Samsung Galaxy S6, S7
Enrollment	5	4
Attempts	5	37 in 24hours
Passcode Requirement	After 48hours	After 24hours

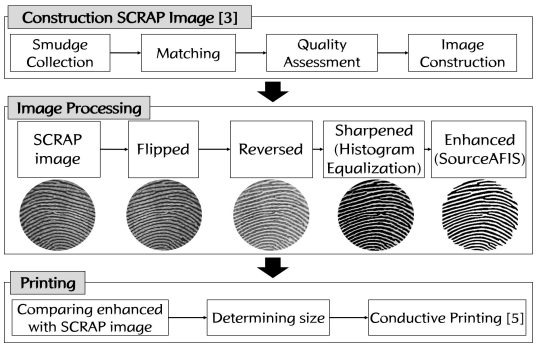


Fig. 2. Attack Procedure

3.3.2 실험 결과

모든 참가자들은 Fig.3.과 같이 Galaxy S7에서 5회의 잠금 해제를 각각 1~2회의 인증 시도만으로 모두 성공하였다. 그러나 Galaxy S8에서는 모든 참가자들이 잠금 해제에 실패하였다. 제조사가 기존 기종의 취약점을 개선한 것으로 보인다.

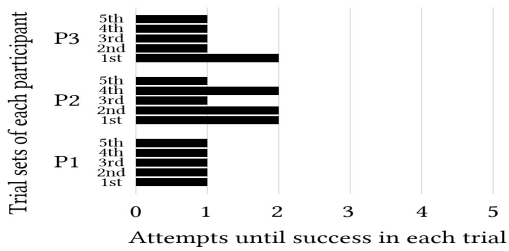


Fig. 3. Attack experiment results (Galaxy S7)

3.4 대응 방법

Lee 등은 스머지로부터 지문 이미지 획득을 방지하기 위한 기술적인 대응 방법으로 다음의 인증 절차를 제안하였다[3].

1) 지문 인증이 필요할 때 터치스크린에 원형 UI를 포함한 슬라이드 바가 나타나며 여기에 손가락을 올려 지문 인증을 수행

2) 지문 입력 후 원형 UI를 왼쪽 또는 오른쪽으로 끌어서 스마트폰을 잠금해제하며 이 과정에서 스머지로부터 인증 지문을 식별할 수 없게 함

이 방법(Fig.4.)은 과거 사용된 '밀어서 잠금해제'에 기초하므로 사용자 적응이 어렵지 않다. 해당 방법은 터치스크린에서 지문 인식이 가능해야 한다는 제약이 있지만 최근 Vivo에서 출시된 X20 Plus

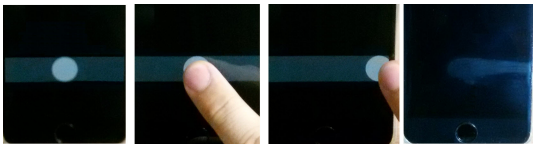


Fig. 4. Mitigation[3]

UD 기종에 'Clear ID'라 불리는, 홈버튼이나 후면 지문 센서 없이 터치스크린에서 지문 인증이 수행되는 기술이 최초로 탑재된 것을 고려한다면 충분히 실현 가능한 방법이다.

Lee 등이 제안한 기술적 대응 방법은 지문 인증 후 스머지를 지문 이미지 획득의 단서를 제거하는 효과 외에도 위조 지문 판별 기능을 가질 수도 있다. 실제 지문이 Fig.1.과 같은 스머지를 남기는 반면 인쇄된 위조 지문은 스머지가 남지 않으므로 스머지 인식 기능을 추가한다면 본 연구에서 제안한 방법에 더 강한 안전성을 갖출 수 있다. 본 연구는 Lee 등이 제안한 대응 방법의 사용자 인식 분석을 수행하였으며 그 절차와 결과가 다음 절에 기술되어 있다.

IV. 사용자 인식 분석

4.1 가설 설정

제안하는 공격 방법을 이해한다면 대부분의 사용자는 지문 스머지를 위협적으로 인식할 것으로 예상하였다. 관찰하고자 했던 점은 사용자들이 이러한 공격을 모르는 상태에서도 알고 있을 때와 같은 수준으로 스머지를 위협적으로 생각하고 있는지 여부였다.

- H1: 제안하는 공격 구조의 인지 여부는 스머지 위협 인식에 양의 영향을 미친다.

사용자들이 3.4절의 대응 방법을 실제로 사용하고자하는 의향을 보인다면 인지된 안전성 및 사용성 중 어디에 영향을 받았는지 분석하기 위해 다음의 가설을 수립하였다. 대응 방법에 대해 사용 의향이 있는 사용자들이 그렇지 않은 사용자들과 같은 수준으로 안전성 또는 사용성을 평가한다면 이는 대응 방법에 결함이 있다는 것을 의미하기 때문이다.

- H2: 대응 방법 사용 의향이 있는 사용자들은 그렇지 않은 경우에 비해 안전성을 높게 평가한다.
- H3: 대응 방법 사용 의향이 있는 사용자들은 그렇지 않은 경우에 비해 사용성을 높게 평가한다.

Table 2. Results of hypothesis test

Hypothesis	Z	p-value	Result
H1	-4.42	〈.001	accept
H2	-2.21	〈.05	accept
H3	-5.02	〈.001	accept
H4	-1.26	.206	reject

대응 방법 사용 의향이 있는 사용자들이라도 안전성과 사용성 모두를 높게 평가하지 않을 수 있다. 예를 들어 안전해보여서 사용 의향이 있다고 답변했지만 기존 지문 인증보다 불편하다고 느끼는 경향이 있을 수 있다. 이 경우 또한 대응 방법의 안전성 또는 사용성에 결함이 있음을 의미한다.

- H4: 대응 방법 사용 의향이 있는 사용자들의 안전성 인식과 사용성 인식에는 차이가 있다.

4.2 설문 설계

설문은 온라인 설문을 활용하여 진행되었다. 참가자들은 다음과 같은 순서로 설문에 응답하였다.

1) 인적 사항: 연령, 성별, 직업, 주로 사용하는 스마트폰 인증 수단, 지문 인식 사용 경험

2) 스머지의 보안 위협 인식: 터치 스크린에 남은 스머지와 이를 확대 촬영한 사진을 보여준 후 이를 얼마나 위협적으로 인식하는지 5-Likert 문항 답변

3) 공격 절차 설명: 촬영된 스머지로부터 인쇄용 지문을 만드는 과정을 사진 예시를 통해 설명받고 이를 인쇄하여 실제로 지문 인증을 통과하는 영상 시청

4) 앞의 2) 단계를 반복

5) 대응 방법 인식: 3.4절의 대응 방법을 사진 및 실제 스마트폰에서의 사용 영상을 활용하여 설명 받고 대응 방법이 기존 지문 인식에 비해 얼마나 불편할 것이라 생각하는지, 지문 위조 공격에 얼마나 더 안전할 것이라 생각하는지 5-Likert 문항 답변

4.3 참가자

61명이 설문에 참가하였으며 그중 남성이 44명(72%)이었다. 연령은 최소 19세에서 최대 52세, 평균 27.2, 표준편차 6.09의 분포를 보였다. 직업은 학생이 28명(46%)로 가장 많았고 공공기관, 판매/영업/서비스직이 각각 7명(11%), 나머지 19명

(31%)의 분포를 보였다. 스마트폰의 주요 인증 수단은 패턴 락 14명(23%), 지문 인증 36명(59%), 기타 방법을 11명(18%)이 사용하였다. 지문 인식 사용 경험에 관해서는 43명(70%)이 사용 중, 8명(13%)이 사용 경험 있음, 10명(16%)이 사용해 본 적 없음의 분포를 보였다.

4.4 결과

제안하는 공격 절차를 설명 받은 전후의 스머지 보안 위협 인식 답변을 비교한 결과, 사용자들은 제안하는 공격을 이해한 후 스머지를 유의하게 더 위협적으로 인식하였다(Wilcoxon signed rank test, $Z=-4.42, p<.001$). 이는 제안하는 공격을 모르면 스머지를 덜 위협적으로 여긴다는 것을 암시한다.

3.4절의 대응 방법이 상용화 된다면 실제로 사용할 의향이 있는지 조사하는 문항에 과반수(31명)가 사용하겠다고 답변하였다. 이들 31명은 제안하는 대응 방법이 기존 지문 인증 방식보다 지문 위조 공격에 안전하다고 여기는 정도가 사용하지 않겠다고 답변한 30명에 비해 유의하게 더 강했으며 (Mann-Whitney's U test, $Z=-2.209, p<.05$) 기존 지문 인증 방식만큼 편리하다고 여기는 정도 또한 유의하게 더 강했다(Mann-Whitney's U test, $Z=-5.014, p<.001$). 또한 이들 31명에 대해 제안하는 방법의 안전성과 사용성 중 더 높게 평가한 항목이 있는지 분석한 결과 안전성과 사용성 인식 사이에는 유의한 차이가 없었다(Wilcoxon signed rank test, $Z=-1.260, p=.208$). 가설 검정의 결과는 Table 2.에 요약되어 있다. 결과는 대응 방법이 기존 지문 인증보다 지문 위조에 더 강함과 동시에 사용성을 크게 낮추지 않는다고 여겨짐을 보여준다.

V. 한계 및 향후 연구

제안한 공격 방법은 Galaxy S7에서만 전도성 인쇄를 활용한 공격이 성공했다. 이러한 한계를 보완하기 위한 방법으로 기존에 널리 알려진 wood glue를 이용한 위조 지문(Fig.5.)에 주목하였다. 먼저 wood glue를 이용한 위조 지문이 최신 스마트폰에도 사용 가능한지 확인하였다. 다양한 제조사의 최신 스마트폰에 지문인증을 10회씩 시도하였고 그 중 성공한 횟수가 Fig.6.에 요약되어 있다. 결과는 wood glue 위조 지문이 사용자의 협조가 있다면 대부분의

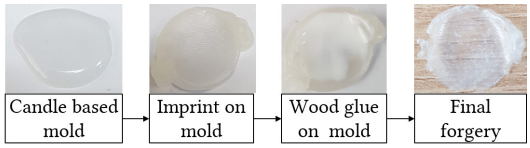


Fig. 5. Forgery using wood glue

최신 스마트폰에 여전히 사용가능함을 보여준다. 사용자의 협조가 필요하다는 제약을 해소하기 위해 아래와 같은 후속 연구가 가능하다.

3절에서의 결과를 통해 스머지로부터 실제 지문 인증 센서를 통과할 수 있는 충분히 정교한 품질의 지문 이미지 복원이 가능함을 확인하였다. 이를 활용하여 3D 프린팅 등으로 위조 지문을 만들 수 있다. 예를 들어 동국대학교 컴퓨터공학과 교수 홍정모 등이 무료로 배포하고 있는 간편 3D 모델링 소프트웨어 Lithopia는 2차원 흑백 이미지로부터 3D 프린팅을 위한 쉬운 모델링을 지원한다. 그러나 이 방법으로는 손가락의 곡면을 포함한 몇몇 특성들이 고려되지 않으므로 위조 지문을 생성하는 과정에서 실제 손가락과 오차가 발생한다. 이러한 오차를 보정하는 방법론을 구축하는 후속 연구가 가능하다.

Fig. 6. Result of wood glue trials

VI. 결 론

본 논문에서는 스마트폰 터치스크린으로부터 지문 스머지를 수집하고[3] 이를 기반으로 지문 인증을 통과하는 방법을 연구하였다. 사용자의 스마트폰으로부터 충분히 좋은 품질의 지문 이미지를 획득한 공격자는 이를 인쇄하여 실제 지문 인증 과정을 통과할 수 있으며 3명의 일반 사용자가 위조 지문을 사용하여 큰 어려움 없이 지문 인증을 각각 5회씩 통과하였다. 61명의 사용자를 대상으로 사용자 인식을 분석하였고 결과는 제안하는 공격 방법이 실제로도 스마트폰 보안에 위협적이며 대응 방법이 이러한 공격

을 방지하면서도 크게 불편하지 않음을 보여준다. 그러나 공격이 제한된 기기에서만 성공적인 결과를 보였으므로 이를 보완하기 위한 후속 연구가 필요하다.

References

[1] Counterpoint, "More Than One Billion Smartphones with Fingerprint Sensors Will Be Shipped In 2018" https://www.counterpointresearch.com/more-than-one-billion-smartphones-with-fingerprint-sensors-will-be-shipped-in-2018/, Mar. 2018.

[2] S. Azenkot and S. Zhai, "Touch Behavior with Different Postures on Soft Smartphone Keyboards," In Proc. of MobileHCI, pp. 251-260, Sep. 2012.

[3] H. Lee, S. Kim, and T. Kwon, "Here Is Your Fingerprint!: Actual Risk versus User Perception of Latent Fingerprints and Smudges Remaining on Smartphones," In Proc. of ACSAC, pp.512-527, Dec. 2017.

[4] A.J. Aviv, K.L. Gibson, E. Mossop, M. Blaze and J.M. Smith, "Smudge Attacks on Smartphone Touch Screens," In Proc. of Woot, Aug, 2010.

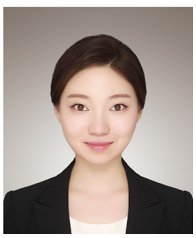
[5] K. Cao and K.J. Anil, "Hacking mobile phones using 2D printed fingerprints," Department of Computer Science and Engineering, Michigan State University, 2016.

[6] SourceAFIS, "SourceAFIS" https://sourceafis.machinezoo.com/net, Aug. 2017.

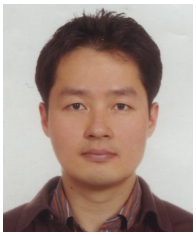
[7] S. Jung and T. Kwon, "Automated Smudge Attacks Based on Machine Learning and Security Analysis of Pattern Lock Systems," Journal of the Korea Institute of Information Security & Cryptology, Vol. 26, No. 4, pp. 903~910.

〈저 자 소 개〉

김 승 연 (Seungyeon Kim) 학생회원
2015년 2월: 세종대학교 응용통계학, 컴퓨터공학 학사 (자연과학대학 수석졸업)
2018년 8월: 연세대학교 정보시스템학 석사
〈관심분야〉 Usable Security, 스마트폰 보안



구 예 은 (Yeeun Ku) 학생회원
2017년 8월: 세종대학교 정보보호학과 학사
2017년 9월~현재: 연세대학교 정보대학원 석사과정
〈관심분야〉 모바일-시스템 보안, 머신러닝



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〉 암호프로토콜, Usable Security, 소프트웨어/시스템보안, 기계학습과보안 등