IoT 환경에서의 생체인증 기반 보안 위협 동향

이정필, 이근호
백석대학교 ICT학부
pil9@kakao.com, root1004@bu.ac.kr

Trend on Security Threats based on Biometric Authentication in IoT Environment

Jeong-Pil Lee, Keun-Ho Lee
Division of Information Communication, BaekSeok University

요 약

생체인증 기술의 발전으로 매년 다양한 인증 기법들이 구현되고 있으며 시장 규모가 급격히 늘어나고 있다. 현재 대부분의 IoT 환경은 생체 인식 등의 사용자 인증 기술을 활용하여 기밀성을 유지하고 있다. 하지만 인증 기술에 사용되는 센서에 인증 우회 기법 등을 통해 오류가 발생하거나 제조사의 실수 등이 포함되는 경우 인증 과정에 대한 보안 위협이 발생할 수 있다. 본 논문에서는 IoT 장비에서 이뤄지는 생체인증의 종류와 종류에 따른 인증 위협요소들을 살펴보고 다중 생체인증 방식을 접목한 대응 프로세스를 알아본다.

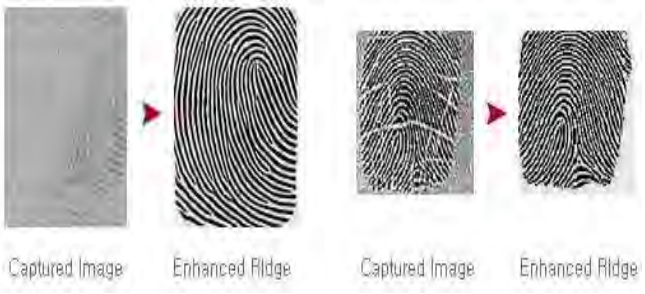
1. 서론

프로세싱 기술과 하드웨어의 발전으로 생체 정보를 활용한 다양한 사용자 인증 기법(생체인증)들이 연구되고 있다. 생체인증 기술은 인간의 생리학적 특성이나 행동상의 특성 등을 기반으로 개개인만의 독특한 특징을 본인확인을 위한 측정단위로 활용하는 기술이다. 사물인터넷(IoT) 기술에도 기밀성 등의 유지를 위해 사용자 인증 기법들이 접목되어 있으며, 특히 생체인증 기술의 장점을 활용한 사용자 인증 기법들이 많이 사용되고 있다[1]. 생체인증 기술에는 대표적으로 음성, 얼굴, 지문, 홍채인식 등이 있으며 각 IoT 장비 제조사 별로 각기 다른 인증 방식을 채택하고 있다. 특히 지문인식 같은 경우 2017년도 기준으로 50%가 넘는 점유율을 차지하고 있으며 IoT 및 센서 장비의 발달로 매년 정확도나 인식률이 개선되고 있다. 하지만 생체인증 정확도의 향상으로 인해 개체에 대해 매우 비슷한 특성을 구분하지 못하거나 센서 장비의 오작동, 인증 프로세스 과정에서 잘못된 인증 알고리즘을 사용하여 보안 위협이 발생할 수 있다. 본 논문에서는 IoT 장비들에 주로 사용되는 생체인증 기술들의 종류와 처리 과정에 관해 설명하고 발생한 보안 위협들에 대해 알아본 뒤 대응방법을 제안하고자 한다.

2. 관련 연구

2.1 지문인증

지문인증은 지문을 인식할 수 있는 전용 센서를 이용해 지문에 대한 디지털 영상을 획득 및 처리하여 사용자를 인식하는 기술이다. 센서마다 상이하긴 하지만 손가락의 전체 정보 또는 일부 정보만 사용하여 대부분 가공된 데이터를 인증 데이터로 사용한다. 다른 생체 인식 기술들보다 센서에 입력하는 과정에 있어서 별다른 데이터가 필요하지 않으며 속도 등의 편의성이 높고 보안성과 인식률이 높아 대부분의 IoT 장비 또는 단말기의 보안 인증 수단으로 채용되어 광범위하게 사용되고 있다.



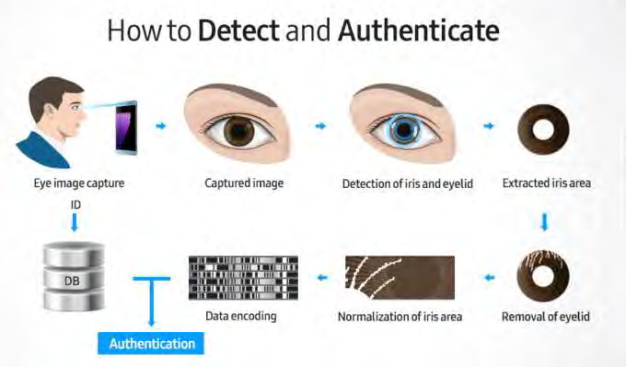
(그림 1) 지문인식 처리 과정

2.2 얼굴인증

얼굴인증은 디지털 이미지를 통해서 사람을 자동으로 식별하는 인증 기술이다. 기존에 등록된 안면 관련 데이터베이스와 살아있는 이미지에 나타나는 얼굴 특징과 비교하여 인증이 이루어진다[2]. 얼굴인증 또한 별다른 데이터가 필요하지 않아 편의성이 높고 인증에 사용할 수 있는 특징점들이 많이 존재하여 생체인증 수단으로 많이 사용되고 있다.

2.3 홍채인식

홍채인식은 홍채의 무늬, 형태, 망막의 모세혈관 분포 등의 패턴을 분석하여 사용하는 인증 기술이다. 보편성, 유일성 등의 바이오 인증 요구사항을 모두 만족하는 인증 과정으로서 높은 인증률로 IoT 장비 등에도 많이 사용되었으나 사용자가 인증을 위해 정확한 위치에 홍채를 맞춰야 하는 등의 번거로움이 있어 편리성이 지문인증 방식보다는 일부 이용율이 낮은 면이 있다. 최근 Samsung Galaxy 시리즈 같은 스마트폰에서는 FoD 기술의 도입 등으로 홍채인식 기술의 채택률이 낮아지고 있다.



(그림 2) 홍채인식 처리 과정(Samsung. “Keeping an Eye on Security: The Iris Scanner of the Galaxy Note7” SamsungNewsroom)

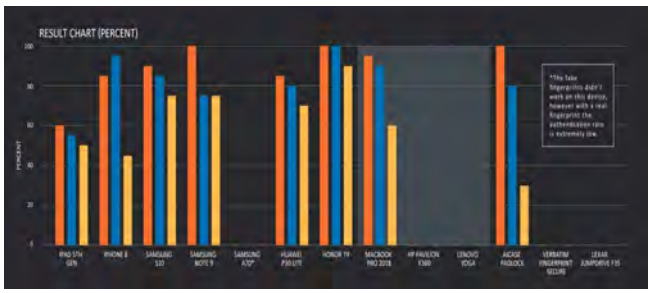
3. 보안 위협

3.1 FoD 우회

지문인식 방식에는 정전식, 광학식, 초음파 방식으로 존재한다. 정전식 광학식, 초음파식으로 발전해 나가는 단계이며 FoD 기술에는 광학식과 초음파식의 인식방식이 도입되고 있다. 하지만 초음파 방식의 인증 방식의 경우 초음파를 통해 지문 굴곡을 측정하여 반사되는 시간을 이용하는 과정에서 보안 위협이 발생할 수 있다. 관련 사례로 Samsung Galaxy 10시리즈에 탑재되었던 초음파 방식의 FOD 기술 관련 생체 인식 프로세스(Fingerprint Software 2.0.24.20 미만 버전)의 처리 과정에서 일부 돌기 패턴을 비정상 지문과 함께 인증하면 지문의 특징점을 추출하는 과정에서 지문 굴곡에 따라서 음파가 반사되는 시간이 지연되게 된다. 해당 시간이 지연되면 반사되는 파장이 왜곡되어 센서에 비정상 데이터가 발생하여 인증 과정의 우회가 가능하다.

3.2 비트 이미지 및 몰드 사용을 통한 우회

지문인증은 지문의 굴곡과 특징점을 추출하여 사용한다. 특히 지문의 굴곡 같은 경우 광원을 통해서만 추출할 수 있는 것이 아닌 유리나 점토와 같은 재질을 통해서도 모양을 쉽게 본뜰 수 있다. 특히 Plasticine과 같은 칼슘, 염 등의 성분이 들어간 재료들을 사용하여 수집하면 형태가 매우 쉽게 남는다. 해당 매체들을 사용하여 수집된 지문 모양의 데이터를 이미지화하고 지문인식 센서에 쉽게 읽힐 수 있도록 각 특징점들을 최적화시킨 뒤 실제 지문 크기와 비슷한 단일 이미지를 만들 수 있도록 동일하게 수집된 다수의 데이터들을 병합한다. 마지막으로 인식률을 올리기 위해 3D 모델링 및 프린팅을 통해 몰드에 복제하여 지문인증 과정을 복제된 데이터로 우회할 수 있다. Plasticine와 같은 모델링 재료를 통하지 않더라도 고성능 DSP 칩이 탑재된 지문인식 센서들을 사용하여 추출된 데이터를 위와 같이 이미지 및 몰드화 시켜서 복제 및 우회가 가능하다[3].



(그림 3) 복제된 몰드를 통한 디바이스별 인증률, 주황색 그래프가 복제된 몰드의 인증률(PAUL RASCAGNERES. “Fingerprint cloning: Myth or reality?” Talos)

3.3 홍채인식 우회

홍채인식은 근적외선을 통해 더그먼 알고리즘을 기반으로 홍채의 명암 패턴을 분석해 디지털 코드로 암호화하게 된다. 하지만 이 과정에서 사람인지 사물인지 물체를 구분하는 과정이 없어 비정상 인증 과정이 발생한다. 관련 사례로 최근 CCC(Chaos Computer Club)에서 실험한 자료[4]를 보면 특정 스

마트폰에 탑재된 홍채인식 센서를 레이저 프린터와 콘택트렌즈만 있으면 우회가 가능하다. 사람의 안면 사진을 촬영하고 눈동자 부분만 확대하여 레이저 프린터로 동공을 콘택트렌즈 크기에 맞게 인쇄한다. 인쇄물 위에 콘택트렌즈를 덧씌워서 홍채인식 센서에 인증하면 인쇄물 상의 홍채의 무늬가 실사용자의 직접적인 무늬인지 검증하는 과정이 없어서 우회가 발생한다.

4. 개선방안

생체인증 보안위협을 궁극적으로 제거하기 위해서는 제 3자에 의해 인증이 발생하는 경우 중 하나인 FAR(False Acceptance Rate) 비율을 낮춰야 한다. 각 생체인증 종류에 따른 평균적인 FAR 값은 다음과 같다.

	지문	홍채	얼굴	정맥(손바닥)
FAR	0.001%~ 0.01%	0.000083% ~0.0001%	1%~1.3%	0.00008%~0.0001%

(표 1) 생체인증 종류 별 FAR 비율 비교 (금융결제원, 바이오인식 기술의 금융서비스 적용현황 및 발전과제)

생체 인증 과정에서 발생하는 대부분의 보안 위협들은 생체 인증 센서의 물리적인 조작보다 인증 프로세스 과정을 무력화 또는 우회를 발생시키는 경우가 대부분이다. 그러나 3-2와 같이 몰드 등의 복제 과정 등을 통해 인증 센서의 데이터 수집과정에서 문제를 발생시키는 경우도 있으므로 KISA 등의 공인된 기관에서 특정 테스트를 통과한 장비를 인증 수단에 사용할 수 있도록 조치해야 한다. 또한 FAR 비율(표1)을 낮추기 위해서는 추가 인증 프로세스를 구현하여 인증 수단을 추가해야 한다. 현재 실 사용되고 있는 생체인증 프로세스에서는 다중 인증 과정이 이루어지지 않고 있으므로 본 논문에서는 다음과 같은 인증방식을 제안한다.

인증 방식	예시
Multiple-Bio	검지 + 엄지 지문
	정면+측면+사용자 패턴
	얼굴 + 지문
	코, 입 특징 + 턱의 각도

(표 2) 다중 생체인증방식 예시

(표2)에서 제시한 Multiple-Bio 방식을 이용하여 각 생체인증 과정에서 보조 인증 프로세스를 추가한다. 예를 들어 지문 인증 프로세스에서 기존처럼 단일 지문을 사용하는 것이 아닌 두 개 이상의 지문을 사용하여 인증하거나, 하나의 지문을 두 개 이상의 방향으로 나누어 인증하고 입력한 방향(패턴)에 대한 사용자 입력 과정을 추가로 진행한다. 초기 생체 인증 설정을 진행할 때 입력된 패턴으로 실시간 데이터(지문)와 함께 추가 인증을 진행한다면 보다 낮은 FAR 비율로 복제된 몰드 등의 우회 기법들을 예방할 수 있을 것이다. 또한, 서로 다른 생체 인증 수단을 동시에 활성화하여 인증을 진행하거나 얼굴인증 과정에서 기존에 많이 사용되는 2D 특징(눈, 입 등)에 턱의 각도나 뼈의 돌출률 등의 3D 데이터를 결합하여 인증 프로세스를 개선한다. 하지만 인증 프로세스가 늘어나게 되면 생체인증 사용 목적에 있어서 편리성 감소 등의 문제가 발생할 수 있으므로 별도의 이상 징후 탐지 프로세스를 추가하여 특정 횟수 이상 등의 시도가 발생하였을 때 (표2)에서 제시한 인증 방식을 추가하는 방향으로 대응할 수 있다.

5. 결론

위와 같이 각 기관이나 그룹들에 의해 지속적으로 생체인증에 대한 우회 기법들이 연구되고 있고 생체인증 관련 하드웨어/펌웨어 제조사의 실수로도 꾸준히 위협이 발생한다. 특히 카메라나 3D 프린터 기술의 발달로 인증 우회를 위해 만들어지는 매체의 해상도가 높아져 최종 인증에 대한 추가 검증 과정이 없다면 쉽게 인증 과정에 대해 우회가 발생할 수 있다. 보안에 있어서 블록체인[5] 등의 기술들과 유사하게 생체인증 시장은 매년 커지고 있으며 특히 금융서비스에도 생체인증 기술을 통한 서비스가 제공되고 있어서 인증 과정에서 보안 위협이 발생할 경우 금전적 손해까지 발생할 수 있다. 생체인증 기술이 탑재된 IoT 장비 또는 기타 디바이스들을 제조할 때 생체인증 센서 등의 안전성을 검증하고 추후 발생할 수도 있는 소프트웨어 결함에 대해 지속적으로 업데이트 가능할 수 있도록 조치해야 한다.

감사의 글

이 논문은 2020년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2020R1I1A3069008)

참고문헌

[1] Gyu-Ho Choi, "Biometrics System Technology Trends Based on Biosignal" Journal of digital convergence, Vol. 15, No. 2, pp.381-391, 2017.

[2] Y. C. Hwang, H. J. Moon, and J. W. Lee, "Face Recognition System Technologies for Authentication System - A Survey", Journal of

convergence society for small and medium business, Vol. 5, No. 3, pp. 9-13, 2015.
[3] “Fingerprint cloning: Myth or reality?.” Talos. last modified Apr 8, 2020, accessed Sep 27, 2020, https://blog.talosintelligence.com/2020/04/fingerprint-research.html.
[4] “Chaos Computer Clubs breaks iris recognition system of the Samsung Galaxy S8.” Chaos Computer Club. last modified May 22, 2017, accessed Sep 27, 2020, https://www.ccc.de/en/updates/2017/iriden.
[5] “A Scheme for Information Protection using Blockchain in IoT Environment” Journal of The Korea Internet of Things Society, Vol. 5, No. 2, pp.33~39, 2019.