사용자 모션 기반 스마트 디바이스 잠금 스킴

변휘림*, 김현우*, 박부광*, 허윤아*, 송은하**, 정영식*
*동국대학교 멀티미디어공학과
**원광대학교 교양교육대학
e-mail : hazzzly@dongguk.edu

Smart Device Locking Scheme based on User Motion

HwiRim Byun*, Hyun-Woo Kim*, Eun-Ha Song**, Young-Sik Jeong*
*Dept. of Multimedia Engineering, Dongguk University
**Dept. of Liberal Arts, Wonkwang University

요 약

스마트 디바이스의 고성능화·초소형화로 사용자의 편리 증대를 위한 다양한 응용 연구가 진행되고 있다. 이러한 응용 연구의 주된 목적은 편리함 및 다양한 서비스 측면을 고려하고 보안 연구는 도외시되고 있어 이와 관련된 개인정보 유출 문제가 발생되고 있다. 이러한 이유로 스마트 디바이스의 다양한 잠금 기법이 개발되었지만 주로 사용되는 잠금 기법의 대부분은 사용자가 Key 로 사용되는 패스워드를 직접 입력하는 과정을 거쳐야 한다. 이 과정에서 Key 가 타인에게 노출될 수 있으며 이는 가장 많이 사용되는 해킹 수법 가운데 하나이다. 본 논문은 스마트 디바이스의 가속도 센서를 활용한 잠금 기법으로 잠금을 해제하는 일련의 추가적인 과정이 없도록 사용자가 디바이스를 손에 쥐고 들어올리는 과정을 Key 로 사용하는 TTU(Take To Unlock)를 제시한다. 타인이 보기에 디바이스의 잠금 여부를 추측하지 못하도록 자연스러운 잠금을 제공하는 것이 TTU 의 목적이며 동시에 사용자가 Key 를 입력해야 하는 추가적인 행위를 최소화 한다.

1. 서론

개인이 소지하는 스마트 디바이스의 종류와 개수가 늘고, 클라우드 · 파일 쉐어링 서비스가 대중화 됨에 따라 개인이 만들어내고 소유하는 데이터가 큰 폭으로 증가하였다. 또한 일상적으로 사용하는 대부분의 서비스가 온라인으로 제공되는 과정에서 개인정보를 포함하는 데이터가 증가하였다. 사용자가 항상 소지하고 다니는 스마트 디바이스의 특성이 개인적인 데이터의 보안에 위험 요소가 되고 있다. 스마트 디바이스를 분실하는 경우 해당 디바이스에 저장된 모든 데이터가 타인에게 공개될 수 있으며 작게는 사진부터 크게는 금융정보까지 유출이 될 가능성이 있다. 이를 막기 위해 관련 업체에서 다양한 스마트 디바이스 잠금 기능을 제공하고 있으며 필수적인 사용을 권고하고 있다. 그러나 스마트 디바이스 잠금은 잠금 해제까지 시간이 소요되어 즉각적인 작업이 불가능하며 항상 사용자가 소지하고 있음에도 자동적으로 잠금이 걸리는 등의 불편함을 야기한다[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12].

이에 본 논문은 사용자가 자연스럽게 디바이스의 잠금을 해제할 수 있는 TTU 를 제시한다. TTU 는 흔들림이 없는 상태에 놓여져 있던 디바이스를 사용하기 위해 자연스럽게 들어올리는 과정 자체의 행동을 비밀번호로 사용한다. 행동을 감지하기 위해 가속도 센서를 사용하며 Outlier 의 제거를 위해 추가적인 데이터 보정을 진행한다. 사용자의 Muscle Memory 에 의해 매번 유사한 동작이 가능할 것으로 가정하는 잠금 방식으로써 기존 잠금 방식과 다르게 추가적인 잠금 해제를 위한 암호 입력 단계가 존재하지 않아 더욱 빠르고 편한 사용이 가능하다.

2. On-Body 와 Rhythm-to-Unlock

2-1. Google On-Body

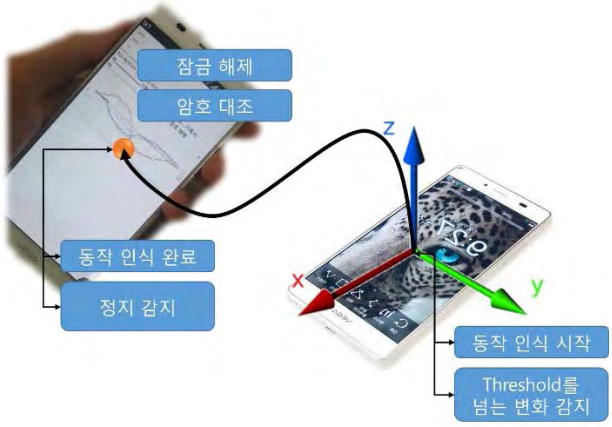
On-Body[12]는 사용자가 계속 디바이스를 휴대하고 있는 동안 잠금 상태로 진입하지 않는 시스템이다. 가속도센서를 사용하여 지속적으로 디바이스 혹은 사용자의 움직임을 확인하여 사용자가 디바이스를 사용중인, 소지하고 있는지를 판단한다. 사용자가 마주하는 디바이스의 잠금 해제 단계를 최소화하여 편의성을 도모한다. 보안의 강화보다는 사용의 편의성을 위한 방법으로 오히려 On-Body 를 미 적용한 상태보다 보안상 취약점이 많을 수 있다. 사용자의 소지여부 판단을 하나의 센서에 의존하며 센싱 데이터가 끊김 없이 입력될 경우 타인을 사용자로 판단할 가능성이 높다.

* 이 논문은 2014 년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2014R1A1A2053564). 또한 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT 연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2015-H8501-15-1014).

2-2. Blackberry Rhythm-to-Unlock

사용자가 디바이스를 두드리는 리듬을 통해 디바이스의 잠금을 해제하는 방식으로 가속도계를 사용하며 디바이스에 전달되는 진동의 패턴을 분석한다[13]. 디바이스의 위치적 상태에 구애 받지 않고 잠금을 해제할 수 있는 강점을 가지고 있으나 패턴 자체가 눈에 띄기 때문에 노출될 수 있는 위험성을 수반한다. 또한 잠금 해제를 위한 추가적인 과정이 있으므로 기존 Pin, Pattern Lock 등에서 단순히 입력의 방식만 바뀐 잠금 기법이라 볼 수 있다.

3. Take To Unlock

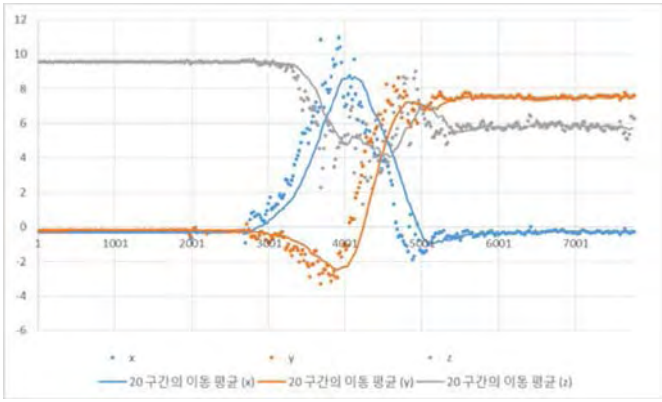


(그림 1) TTU 처리 과정

그림 1 은 TTU 잠금 해제의 프로세스 과정을 나타낸 그림이다. TTU 는 디바이스가 잠금 상태일 경우 지속적으로 가속도계를 사용하여 움직임을 감지한다. 사용자가 디바이스들 집어 들어 가속도계에서 움직임이 감지되는 순간부터 동작인식 과정이 시작된다. 동작인식 과정은 사용자가 디바이스를 집어 들어 주시하기까지의 시간 동안 가속도를 기록하며 이동평균을 사용하여 보정을 거친다. 이렇게 보정된 데이터는 잠금을 풀기 위한 Key 로 사용하며 사용자가 움직임을 멈추면 디바이스는 가속도계를 통해 정지를 감지하고 동장인식 과정을 마친다. 위 과정을 통해 얻어진 Key 가 기존에 설정되어있는 Key 와 다르지 않다면 디바이스의 잠금이 해제되고, 일정 임계치 이상 오차가 생긴다면 잠금 해제에 실패하여 다시 동작인식 과정으로 진입한다..

3.1 Key

TTU 는 움직임이 없는 정적인 상태의 디바이스를 집어 화면을 응시하는 과정의 움직임을 Key 로 사용한다. 이 과정 동안 가속도 센서 기반 X, Y, Z 차원 축의 센싱 데이터를 입력 받는다. 이 데이터는 가속도 센서의 민감도 문제로 인해 많은 수의 Outlier 가 내제되어있어 Raw data 상태로 사용하기에는 신뢰에 어려움이 따르기 때문에 추가적인 보정 작업이 이루어져야 한다. 데이터의 특성상 함수의 차수를 예측할 수 없고, 그 특성을 선형으로만 나타내기에는 정확도에 한계가 있으며 데이터를 최대한 빠르게 실시간으로 처리해야 하기 때문에 이동평균법(Moving Average)을 사용해 Raw data 를 보정한다. 결과적으로 이동평균법을 통해 보정된 데이터를 TTU 의 Key 로 사용한다.



(그림 2) Raw Data 및 Moving 평균 그래프

그림 2 는 가속도 센서에 의해 입력된 Raw 데이터와 이동평균법에 의해 보정된 데이터를 나타낸 그래프이다. 그래프의 Y 축은 가속도센서의 데이터 값이고 X 축은 시간의 흐름을 나타내며 최소 단위는 20ms 이다. 작은 점들은 단위 시간마다 센싱된 데이터의 수치이고 실선은 해당 데이터들을 n=20 으로 처리한 이동평균이다. 그림 2 를 통해 Outlier 를 최소화시킴을 확인할 수 있다.

3.2 Threshold

TTU 는 사용자의 Muscle Memory 에 의존하는 잠금 기법으로 사용자가 완벽히 동일한 행동을 보일 수 없을 것이라는 가정을 한다. 따라서 Key 와 센싱 데이터가 수치상 정확히 같지 않을 것이라 예상하고 오차 허용 범위 임계치를 정의한다. 임계치의 범위는 사용자 마다, 동작에 따라서 편차를 보일 수 있다. 따라서 TTU 는 Key 마다 각기 다른 임계치를 사용한다. 임계치는 사용자가 Key 를 설정하는 과정에서 동일한 Key 를 여러 번 반복하게 하여 이 Key 들의 평균 오차를 임계치로 설정한다.

$$\text{임계치} = \frac{1}{n}\sum_{i=0}^{n} M_i - N_i \qquad (1)$$

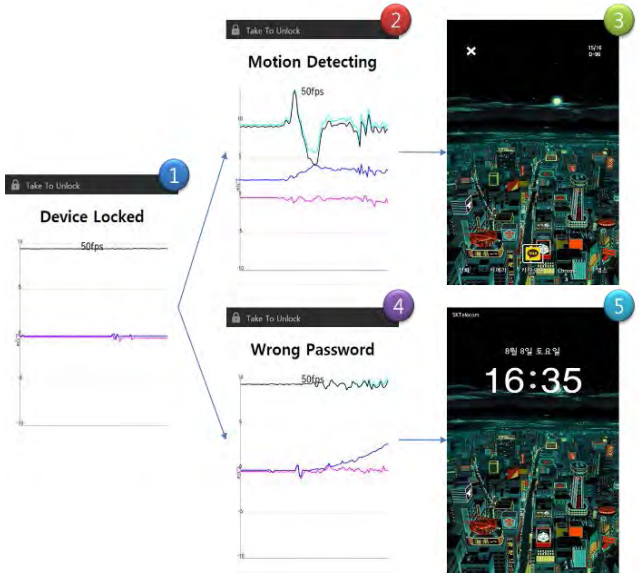
식 (1)은 TTU 의 임계치를 구하기 위한 공식으로 n 은 데이터의 개수 M 과 N 은 서로 다른 Key 를 의미한다.

3.3 Unlocking Process

디바이스에 움직임이 감지되면 TTU 의 잠금 해제 과정이 시작된다. 사소한 움직임이나 잔 떨림에 의한 시작을 막기 위하여 X, Y, Z 축에서 함께 움직임이 보여야 프로세스로 진입한다. TTU 의 잠금 해제 프로세스는 센싱 데이터의 보정과 동시에 처리된다. 계산된 보정 데이터를 설정되어있는 Key 와 비교한다. 데이터의 주기는 20ms 로 설정되어있으며 사용자의 반응 민감도 여하에 따라 설정이 가능하도록 구현되었다. 주기마다 데이터를 비교하며 만약 허용 오차를

벗어나는 차이가 나타날 경우 잠금 해제 실패로 간주한다. 여기서 Key 와 보정 데이터의 허용 오차는 임계치 값에 기반한다. 저장된 Key 의 길이만큼의 데이터 비교가 끝나면 일치하는 동작으로 보고 잠금이 해제된다. TTU 의 목표는 자연스러운 동작에서 파생되는 잠금 해제 방법이기 때문에 만약 잠금 해제에 실패할 경우 다시 TTU 프로세스로 진입하지 않고 PIN, 패턴락 Pattern Lock 과 같은 보조적 잠금 해제 방법으로 진입한다.

4. TTU 의 구현



(그림 4) TTU 잠금 및 잠금 해제 과정

그림 4 은 TTU 를 안드로이드 기반으로 실제 구현한 화면이다. 그림 4 내의 ①은 TTU 를 사용하여 디바이스가 잠겨 있는 상태를 나타낸다. 그림 4 내의 ②는 디바이스의 움직임을 감지하여 가속도계의 데이터가 센싱되는 상태로 Key 가 입력되어 처리되는 상태를 나타낸다. 그림 4 의 ③은 올바른 Key 가 입력되어 TTU 의 잠금이 해제된 상태를 나타낸다. 그림 4 의 ④는 TTU 의 Key 와는 다른 움직임이 입력된 상태를 나타낸다. 그림 4 의 ⑤는 지속적인 Key 의 불일치가 일어날 경우에 TTU 의 작동은 정지되고 다른 잠금 기능으로 넘어간 상태를 나타낸다.

5. 결론 및 향후 연구

TTU 는 디바이스 잠금으로 파생되는 불편함을 최대한으로 줄이고 잠금 성능에 저하가 없는 방식으로 설계되었다. TTU 의 Key 로 입력되는 동작의 길이와 범위에 제한이 없어 길이는 디바이스 메모리의 한계까지 이고 동작의 범위는 디바이스 센서의 한계치까지이다. 따라서 Key 는 무수히 많은 조합이 가능하다.

향후에는 단순히 디바이스에 움직임이 없는 정적인 상태에서 외의 상태에서 사용이 가능한 잠금 기능을 구현하고자 한다. 또한 아직까지는 설정된 Key 와 입력하는 Key 의 오차를 단순히 임계치와 비교하는 방법을 사용하지만 상황과 시간에 따라 사람의 동작이 작은 범위 내에서 달라질 수 있는다는 점을 고려하여 이러한 오차를 인식하고 비교할 수 있는 알고리즘을 구현하여 정확도를 향상시키고자 한다.

참고문헌

[1] Muhammad Shahzad, Alex X. Liu, Arjmand Samuel, “Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures – You can see it but you can not do it,” MobiCom '13 Proceedings of the 19th annual international conference on Mobile computing & networking, pp. 39-50, Sep. 2013.

[2] Ahmed Sabbir Arif, Michel Pahud, Ken Hinckley, Bill Buxton, “A Tap and Gesture Hybrid Method for Authenticating Smartphone Users,” MobileHCI '13 Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services, pp. 486-491, Aug. 2013.

[3] 박동규, 정정수, “모션 캡쳐를 이용한 기타 리듬게임,” 한국정보통신학회논문지, 17 권, 5 호, pp. 1106-1112, 2013.

[4] Tetsuji Takada, Yuki Kokubun, “MTAPIN: multi-touch key input enhances security of PIN authentication while keeping usability,” International Journal of Pervasive Computing and Communications, Vol. 10, Issue 3, pp. 276-290, 2014.

[5] Seongil Lee, Kyohyun Song, Jiho Choi, “Access to an Automated Security System Using Gesture-Based Passwords,” Network-Based Information Systems (NBiS), 2012 15th International Conference on, pp. 760-765, Sep. 2012.

[6] 김현수, 오경헌, 이건영, "모션인식 게임을 위한 스마트폰 센서 데이터 처리," CICS 2013 정보 및 제어 학술대회, pp. 292-293, 2013.

[7] 이용철, 이칠우, "센서 정보를 활용한 스마트폰 모션 인식," 멀티미디어학회논문지, 17 권, 12 호, pp. 1437-1445, 2014.

[8] 이광형, 신동규, 신동일, "직관적인 핸드 모션에 기반한 NUI/NUX 프레임워크," 인터넷정보학회논문지, 15 권, 3 호, pp. 11-19, 2014.

[9] Nixon, K.W., Xiang Chen, Zhi-Hong Mao, Yiran Chen, Kang Li, "Mobile user classification and authorization based on gesture usage recognition," Design Automation Conference (ASP-DAC), 2013 18th Asia and South Pacific, pp. 384-389, Jan. 2013.

[10] 민경보, 정의철, "NUI 디자인을 위한 자연스러운 제스처 수집 방안 제안," 한국디자인학회 2014 봄 국제학술대회, pp. 86-87, 2014.

[11] Lei Yang, Yi Guo, Xuan Ding, Jinsong Han, Yunhao Liu, Cheng Wang, Changwei Hu, "Unlocking Smart Phone through Handwaving Biometrics," Mobile Computing, Vol. 14, Issue 5, pp. 1044-1055, 2014.

[12] Google On-Body Detection. https://support.google.com/nexus/answer/6093922?hl=ko

[13] Kevin Orr. 2006. 『System and method for locking and unlocking access to an electronic device』.US8125312 B2. Research In Motion Limited. G08C19/00.